Installation Manual

GuardNVR

Let's make things safer!

Contents

CONTENTS **2**

1 INTRODUCTION **4**

1.1 EQUIPMENT CHECKLIST 5
1.2 MINIMUM SYSTEM REQUIREMENTS 5

2 GETTING STARTED **6**

2.1 WORK SPACE CONDITIONS 6
2.1.1 General conditions *6*
2.1.2 Placement conditions *7*
2.2 GUARDNVR IIS SPLIT 8
2.3 INSTALLING GUARDNVR 12
2.3.1 Trial mode *15*
2.4 STARTING UP FOR THE FIRST TIME 16
2.4.1 Desktop icons overview *16*
2.4.2 Logging on to GuardNVR server *17*
2.4.3 Changing password *17*
2.4.4 Setting time *17*
2.4.4.1 Through GuardNVR Web Application 18
2.4.4.2 Through Operating System (XP or Vista) 18
2.4.4.2.1 Changing time zone 18
2.4.4.2.2 Time synchronization 19
2.4.5 Changing keyboard settings *19*
2.4.6 Adjusting screen resolution *21*
2.5 GUARDNVR IN THE NETWORK 22
2.5.1 Network overview *22*
2.5.2 Connecting GuardNVR to the local network *23*
2.5.3 Assigning IP address *23*
2.5.4 Firewall configuration *24*
2.5.5 Connecting a client *26*
2.5.5.1 Minimum client requirements 26
2.5.5.2 Client configuration 27
2.5.6 Connecting GuardNVR to the Internet *29*
2.5.6.1 Creating a network connection 29
2.5.6.2 Router and firewall 30
2.5.6.2.1 Configuring router 30
2.5.6.2.2 Configuring firewall 31
2.6 TESTING GUARDNVR 34
2.6.1 Local client test *34*
2.6.2 Connection test *34*
2.6.3 Remote client test *35*

3 UPGRADING & RESTORING GUARDNVR **36**

3.1 UPGRADING GUARDNVR SOFTWARE 36
3.2 SAVING AND RESTORING CONFIGURATION 36

4 ADVANCED TOPICS **37**

4.1 EXTENDING STORAGE SPACE 37
4.1.1 Adding hard disk *37*
4.1.2 Configuring added hard disk *38*
4.1.2.1 Multiple Logical Disks 40
4.1.2.2 Single Disk Extension 42
4.2 VIDEO CLIENT COMPONENT (ACTIVEX) 47
4.3 CHANGING NETWORK PORTS 49
4.3.1 Changing GuardNVR video ports *49*
4.3.2 Changing TCP port *49*
4.3.3 Changing remote desktop port *50*

4.4 GUARDNVR POWER ON AFTER POWER FAILURE 50
4.5 CONFIGURING AUDIO OVER THE INTERNET 50
5 STORAGE / BANDWIDTH CONSIDERATIONS 52
5.1 TERMINOLOGY AND BASIC VIDEO TECHNOLOGY 52
5.2 FACTORS THAT INFLUENCE BIT RATE AND VIDEO QUALITY 54
5.2.1 Compression technique (codec) 54
5.2.2 Resolution 55
5.2.3 Frame rate 56
5.2.4 "Differential" live streaming 57
5.2.5 Activity detection for storage 57
6 SECURITY POLICY 58
6.1 PROPER USE OF GUARDNVR 58
6.2 SECURITY POLICY 59
6.2.1 Password policy 59
6.2.2 Windows security updates 61
6.2.3 Network security 61
6.2.3.1 Dedicated network versus integration with the corporate network 61
6.2.3.2 Connecting GuardNVR to the Internet 62
6.2.3.3 Limiting the number of protocols 62
6.2.3.4 Firewall 62
6.2.3.5 Allowing only known clients 63
6.2.3.6 Securing the applications 63
6.2.3.7 VPN 63
6.2.4 Other types of access 64
6.2.5 3rd party security tools 64
6.3 ERROR RECOVERY MECHANISMS 64
7 TROUBLESHOOTING 65
7.1 PROBLEM SOLVING PROCESS 65
7.1.1 Preliminary checklist 65
7.1.2 Analyzing the problem 66
7.2 SOLUTIONS FOR COMMON PROBLEMS 67
7.2.1 Start up problems 67
7.2.2 Monitor problems 69
7.2.3 Windows logon problems 69
7.2.4 Remote connection problems 70
7.2.5 Camera problems 71
7.2.6 GuardNVR software problems 71
7.3 IF YOU NEED FURTHER ASSISTANCE 73
7.3.1 Before you call 73
7.3.2 Collecting the necessary information 73
7.3.3 How to contact Quadrox 74
7.3.4 How to allow remotely access to your GuardNVR by Quadrox support 74
8 APPENDICES 75

1 Introduction

GuardNVR is a unique digital video surveillance solution, which combines three major functions in one Network Video Recorder (NVR) or Digital Video Recorder (DVR): local digital recording, multiplexing and simultaneous transmission of the video via existing networks (TCP/IP). To a standard GuardNVR, up to 20 cameras can be permanently recorded while multiple operators at different locations on the network are accessing the GuardNVR network video server.

Being a networked device, GuardNVR utilizes two basic principles of the Internet/Intranet technology:

- GuardNVR works over the TCP/IP network protocol, which provides maximum connectivity. This means that the existing computer network infrastructure can be used eliminating extra installation expenses.
- GuardNVR uses a web-based user interface to view live images, recordings, etc. More specific it uses Microsoft **Internet Explorer.**

Remote and Local Monitoring

To remotely monitor the connected cameras, the GuardNVR uses Web Browser technology. To locally monitor video, the GuardNVR also provides a local interface via a PC monitor directly connected to the GuardNVR. This local interface allows an operator to see live video from the connected cameras without the need for additional client computers on a network.

Continuous Activity-Based Recording

By default, a GuardNVR continuously records all images from all the connected cameras based on activity detection. In this case, only movement is recorded. If there is no movement, no recording takes place. If necessary, the GuardNVR can be set to record continuously.

Intelligent Storage Option

GuardNVR uses a first-in/first-out (FIFO) overwrite principle. Once the disk is full, the oldest images are overwritten.

Semi-Continuous recording (recording based on activity detection) allows a GuardNVR to store pre- and post-alarm video. Pre- and Post-alarm images are often more important than the

images at the time of the alarm event itself. Up to 5 minutes of pre- and post-alarm video can be stored per event.
GuardNVR makes a distinction between common activity recordings and pre/post alarm recordings. In the way that, alarm recordings have a higher storage priority and will not be overwritten by non-alarm recordings.

The GuardNVR is operational even when no live monitoring occurs. While the GuardNVR continuously records images from all the cameras, video is transmitted from the server to the client **only** when an Internet browser is connected to GuardNVR and someone is live-viewing images from one or more cameras.

1.1 Equipment checklist

The following items you'll find on the GuardNVR installation CD/DVD.

- GuardNVR4 Video security software suite
- Adobe Acrobat Reader 8.0 or higher
- GuardNVR Installation manual in PDF format
- GuardNVR User manual (=WebCCTV User manual) in PDF format
- Remote POS Monitor Guide in PDF format
- Alarm Component Installation manual in PDF format

1.2 Minimum system requirements

The following system components are the minimum requirements for a proper GuardNVR operation:

Hardware
- Intel Dual Core or higher
- 2048 MB RAM
- 256 MB RAM on the video card

Operating System
- Windows XP Pro Service Pack 3
- Windows Vista
- Windows 7

64-bit Operating Systems are not yet supported.

Software and MS Windows components
- Internet Information Services (IIS)
- Internet Explorer 7 or higher
- DirectX 9.0c

Media players and codecs
- Windows Media Player 11
- Windows Media Formats 11

Some useful downloads are available in the **System Downloads** menu. See the User Manual for more information.

2 Getting started

This chapter provides information to get you started using your GuardNVR. It covers the following topics:

- Work space conditions.
- GuardNVR IIS Split.
- Installing GuardNVR.
- Starting up for the first time.
- GuardNVR in the network.
- Testing GuardNVR.

2.1 Work space conditions

Establishing a comfortable and appropriate work site and placement of the GuardNVR is important to you and your GuardNVR. Proper ambient conditions should also be maintained for the GuardNVR's operation. This section discusses the following topics:

- General conditions
- Placement conditions

2.1.1 General conditions

Carefully read the following guidelines:

- Make sure there is adequate space around the GuardNVR for proper ventilation. Leave ample ventilation room for the cooling fan. Do not block the vents. If your unit is placed in a lockable enclosure, be sure to use only enclosures that are fan cooled and ensure that the fan is operational. It is also a good practice to place the GuardNVR in the middle of the cabinet to maximize air flow.
- Make sure the AC power cord connects to an outlet that is close to the GuardNVR and easily accessible.
- Make sure the Ethernet cable is correctly connected and is laid properly, without strain.
- The temperature should be 5 to 40 °C (41 to 104 °F) and the relative humidity should be 5 to 95 %.
- Avoid areas where rapid or extreme changes in temperature or humidity may occur.
- Keep the GuardNVR free of dust, moisture and exposure to direct sunlight and away from heat sources, such as electric heaters.
- Do not use the GuardNVR near liquids or corrosive chemicals.
- Some components in the unit, including data storage media, can be damaged by magnets. Do not place the GuardNVR near magnetic objects or bring magnetic objects close to the GuardNVR. Be careful of objects, such as stereo speakers, that produce strong magnetic fields during operation.

2.1.2 Placement conditions

Position the GuardNVR and peripheral devices to provide comfort and safety.

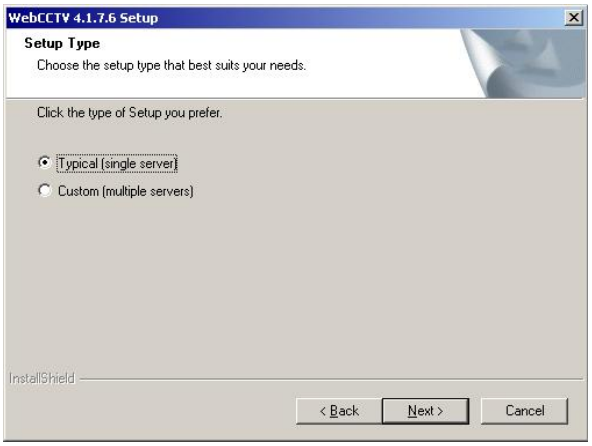
- Set the GuardNVR on a flat surface at a comfortable height and distance. If the monitor is connected it should be no higher than eye level to avoid eyestrain.
- Do not place any liquid containers on the GuardNVR system, such as water, coffee, or beverage. If liquid is poured onto the GuardNVR, it can cause a system malfunction or fire.
- Prevent the power cable from being severely bent by a heavy object. This may cause fire.
- Clean the dust around the GuardNVR on a regular basis. When cleaning the system, always use a dry cloth. Do not use wet cloth or other organic solvents. This may damage the surface of the GuardNVR and may cause system malfunction or electric shock.
- When pulling the power cable from the plug, do so gently. Do not touch the plug with wet hands and avoid using the plug if the holes on the outlet are too loose. This may cause fire or an electric shock.
- Do not attempt to disassemble, repair, or modify the GuardNVR yourself. It is extremely dangerous due to high voltage running through the GuardNVR. This may cause fire, electric shock, or serious injuries.
- Keep at least 15cm (6inches) between the back of the GuardNVR and a wall for the cables connected into the GuardNVR. Otherwise, cables may be bent, damaged, or cut. This may cause fire, electric shock, or injuries.
- The power outlet must be grounded, and the voltage range must be within 10% of the voltage rate. Do not use the same outlet with a hair dryer, iron, refrigerator, or any heating appliances. This may cause fire, heating, and an electric shock.
- Do not place any heavy object on the GuardNVR system. This may cause system malfunction.
- The GuardNVR can be damaged from a strong impact or vibration. Avoid throwing objects within the vicinity of the GuardNVR.

2.2 GuardNVR IIS Split

As stated before, the GuardNVR application is a real web application which increases the flexibility and connectivity considerably. This web application is managed by IIS (Internet Information Services) which is installed on a computer of choice which can run IIS.

Versions prior to version 4.0.8.0 only have the ability to install IIS on the Video Server itself.

By having the option to install the web application (by using IIS) onto a computer of choice, it is possible to simplify the connection and scalability of the global security installation as the server itself and the web application don't have to be installed on the same unit.



Setup Type Selection Screen

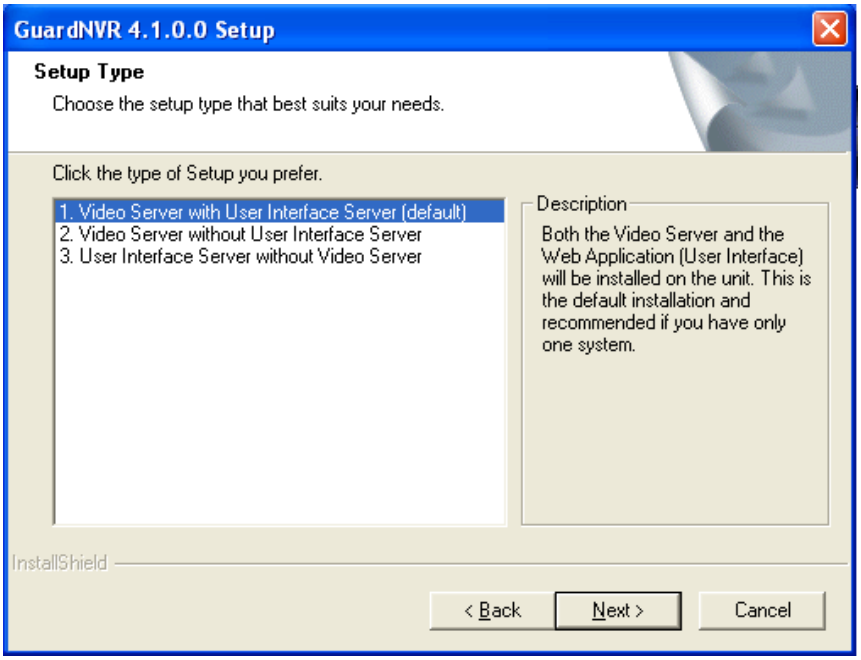
There are three possible options:

- **Video Server with User Interface Server (default)** – Both the video server and the web application will be installed on the unit. Option **Typical (single server)** or first option in the Custom menu.

This is the default installation and recommended if you have only one GuardNVR system.

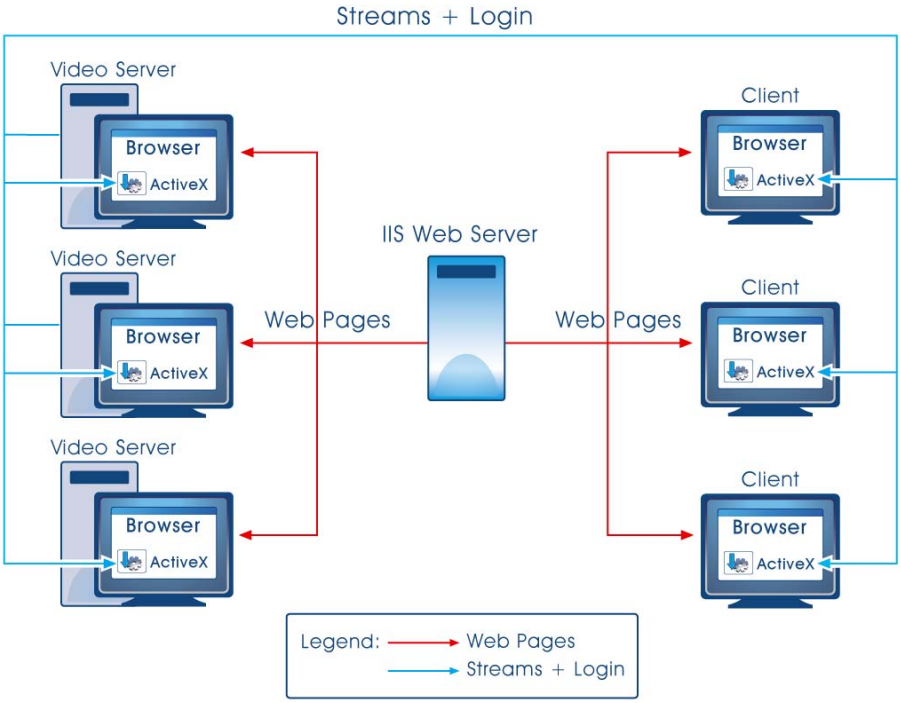
- **Video Server without User Interface Server –** Only the Video Server is installed. This means you have installed the Web Application (User Interface) on another system. Option **Custom (multiple severs).**
- **User Interface Server without Video Server –** Only the Web Application is installed. Ideally this web application will be used as the central web application for all the GuardNVR systems in your network. Option **Custom (multiple severs).**

You can choose one of the three options during the installation of your system by selecting **Custom**. Ask your installer for more information if you didn't install the system yourself.

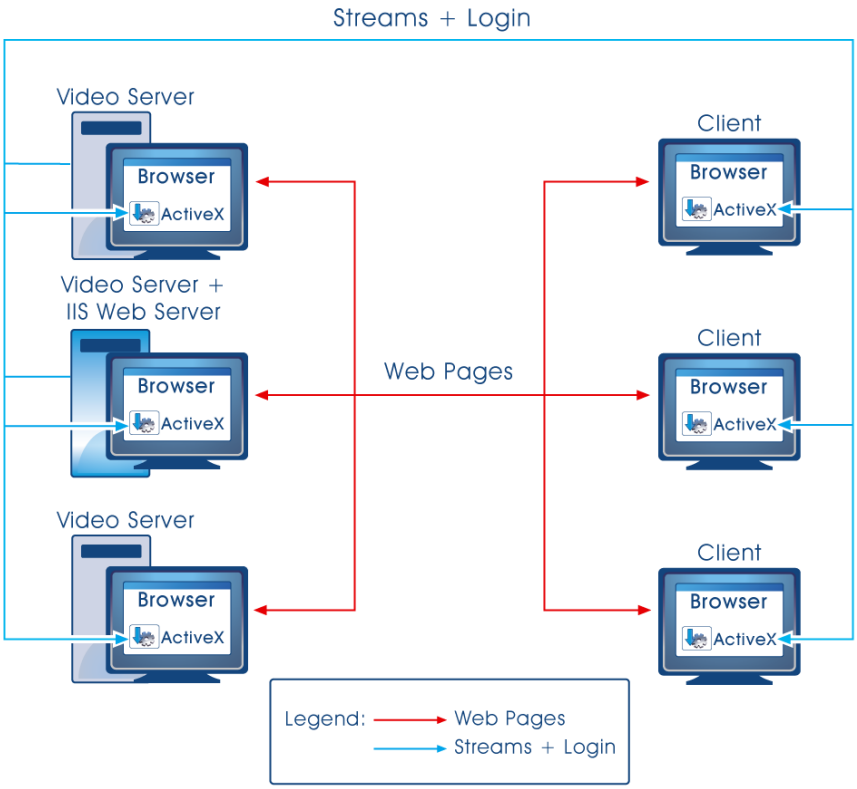

GuardNVR 4.1.0.0 Setup
Setup Type
Choose the setup type that best suits your needs.
Click the type of Setup you prefer.
1. Video Server with User Interface Server (default)
2. Video Server without User Interface Server
3. User Interface Server without Video Server
Description
Both the Video Server and the Web Application (User Interface) will be installed on the unit. This is the default installation and recommended if you have only one system.
InstallShield
< Back
Next >
Cancel

Setup Type Selection Screen

The following pictures give you an idea how it works:



Centralized IIS Server on separate unit

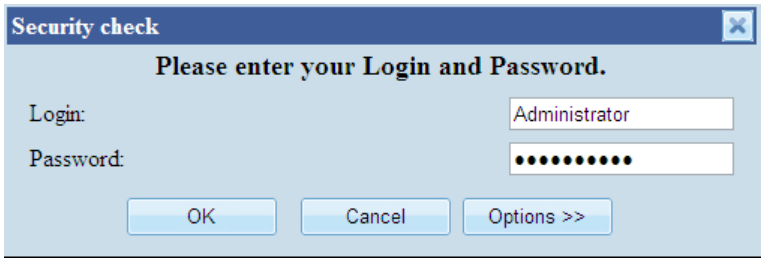


Centralized IIS Server on a Video Server

Let us explain how this works in reality!

If you have multiple Video Servers installed and have installed a centralized IIS server (On one of the Video Server or even on a separate PC), then you can connect to each Video Server by connecting first to the centralized Web Application by typing the IP of that unit. At that time you can choose which server you want to connect to in the network from the extended logon screen. In this case you only need to remember one IP address to connect to all your GuardNVR servers.

This means that when you connect to a Video Server that also has the Web Application installed you will need the basic logon screen shown below:

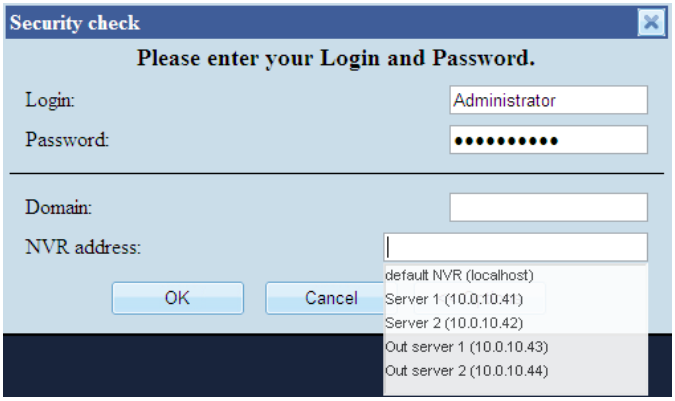


Basic Logon Screen

If you want to connect through the centralized Web Server, you have to use the extend logon screen by clicking **Options**. There you select or type the video server IP or DNS name:

For more information about the configuration of this setup, see chapter **3.3.7. Network Video Recorders** of the GuardNVR User Manual.

You can choose which server you want to use as the default server to connect to. For more information, see chapter **3.3.7. Network Video Recorders** of the GuardNVR User Manual.

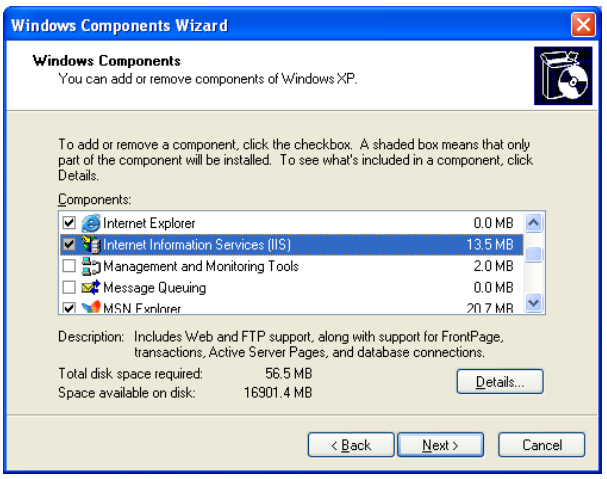


Extended Logon Screen

When you choose to install and manage the Web Application on your GuardNVR server or one of your GuardNVR servers, IIS has to be installed as stated before.

If IIS is not yet installed, follow the steps below:

1. Switch on your computer and login as an Administrator.
2. Insert Windows installation CD into your CD/DVD drive.
3. Click **Start->Settings->Control Panel->Add/Remove Programs**. Choose there **Add/Remove Windows Components** tab.


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Explorer 0.0 MB
Internet Information Services (IIS) 13.5 MB
Management and Monitoring Tools 2.0 MB
Message Queuing 0.0 MB
MSN Explorer 20.7 MB
Description: Includes Web and FTP support, along with support for FrontPage, transactions, Active Server Pages, and database connections.
Total disk space required: 56.5 MB
Space available on disk: 16901.4 MB
Details...
< Back
Next >
Cancel

Windows Components Wizard Screen

4. Select **Internet Information Services (IIS)** item in the window that appears and click **Next**.

5. After installation is completed click **Finish**.

2.3 Installing GuardNVR

To install GuardNVR follow the steps below:

1. Insert GuardNVR installation CD/DVD into your CD/DVD-drive.
2. If Autorun is disabled go to **My Computer** and double-click on the drive icon that corresponds to your CD-ROM.
3. Wait while installation procedure is loading and click **Next** button in the screen that appears.
4. Carefully read the **License Agreement** and click **Yes** if you agree.
5. For a default installation, select Typical. For a custom installation, select Custom. Click next. If you selected custom, you need to define the type of installation in the window that appears and click **Next**.

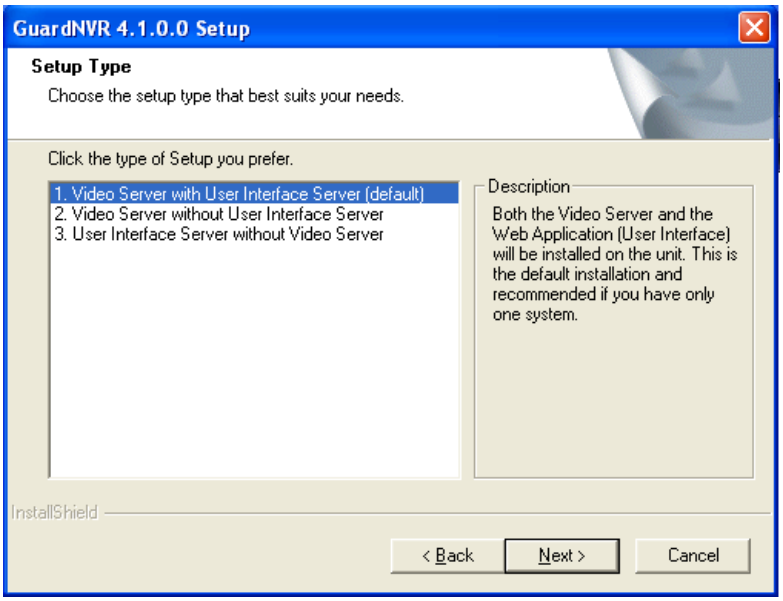
   There are three possible options:

   - **Video Server with User Interface Server (default)** – Both the video server and the web application will be installed on the unit.

This is the default installation and recommended if you have only one GuardNVR system.

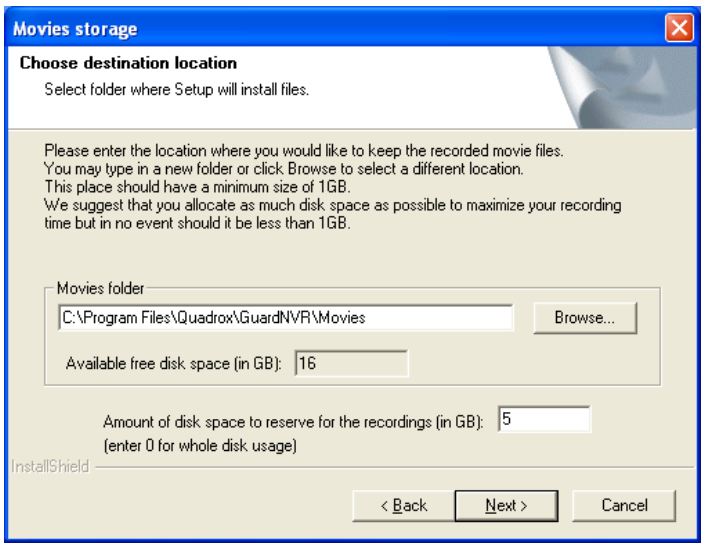
   - **Video Server without User Interface Server –** Only the Video Server is installed. This means you have installed the Web Application (User Interface) on another system.
   - **User Interface Server without Video Server –** Only the Web Application is installed. Ideally this web application will be used as the central web application for all the GuardNVR systems in your network

You have to choose one of the three options during the installation of your system. Ask your installer for more information if you didn't install the system yourself.


GuardNVR 4.1.0.0 Setup
Setup Type
Choose the setup type that best suits your needs.
Click the type of Setup you prefer.
1. Video Server with User Interface Server (default)
2. Video Server without User Interface Server
3. User Interface Server without Video Server
Description
Both the Video Server and the Web Application (User Interface) will be installed on the unit. This is the default installation and recommended if you have only one system.
InstallShield
< Back
Next >
Cancel

Setup Type Selection Screen

6. Choose the destination where GuardNVR will be installed and click **Next**. If the folder not yet exists, it will ask to create it. Click **Yes** in order to create it.
7. Choose the destination for movie storage in the next window.


Movies storage
Choose destination location
Select folder where Setup will install files.
Please enter the location where you would like to keep the recorded movie files.
You may type in a new folder or click Browse to select a different location.
This place should have a minimum size of 1GB.
We suggest that you allocate as much disk space as possible to maximize your recording time but in no event should it be less than 1GB.
Movies folder
C:\Program Files\Quadrox\GuardNVR\Movies
Browse...
Available free disk space (in GB):
16
Amount of disk space to reserve for the recordings (in GB):
5
(enter 0 for whole disk usage)
InstallShield
< Back
Next >
Cancel

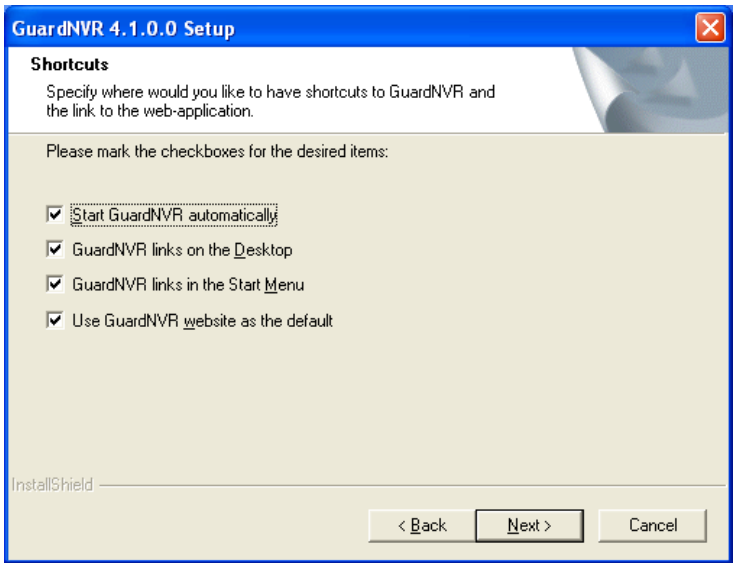
Movies Storage Screen

It is recommended to make a separate disk partition to store movies.

8. In the same window you are able to choose the amount of the disk space reserved for movie storage, by default 1 GB (Gigabyte) is specified.

It is recommended to reserve as much disk space as possible for movies. This value defines how fast GuardNVR will rewrite the stored video footage.

9. Click **Next**.
10. Choose the appropriate GuardNVR shortcuts by selecting the corresponding checkboxes. Click **Next**.


GuardNVR 4.1.0.0 Setup
Shortcuts
Specify where would you like to have shortcuts to GuardNVR and the link to the web-application.
Please mark the checkboxes for the desired items:
Start GuardNVR automatically
GuardNVR links on the Desktop
GuardNVR links in the Start Menu
Use GuardNVR website as the default
InstallShield
< Back
Next >
Cancel

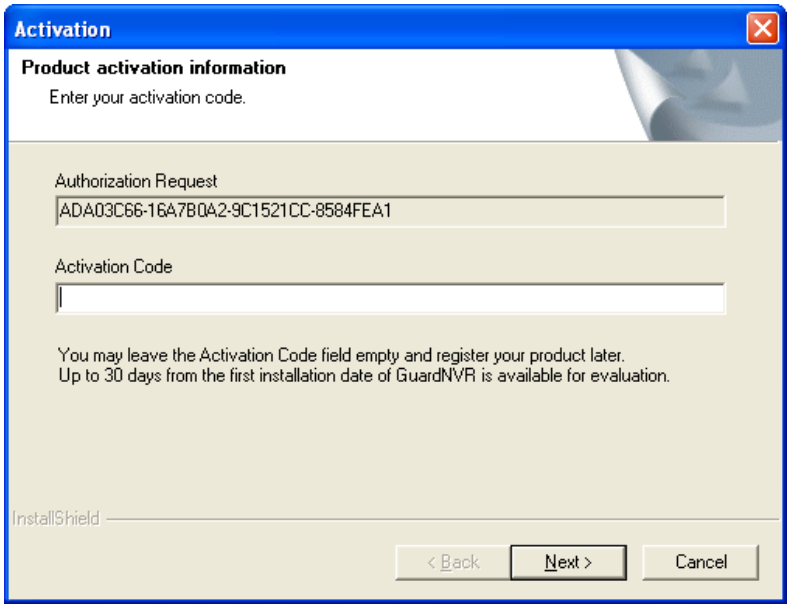
Shortcuts Screen

11. In the last window click **Next** once more in order to start the installation.

The installation process will ask you to allow making some changes in the Windows FireWall. The following ports will be opened automatically:

1. **TCP** Port 80: httpa
2. **TCP** Port 1518: GuardNVR control connection
3. **UDP** Ports 4096 till 4223: GuardNVR video streaming

12. Enter your **Activation Code** that is generated based on the Authorization **Code** after initial installation and click **Next**.


Activation
Product activation information
Enter your activation code.
Authorization Request
ADA03C66-16A7B0A2-9C1521CC-8584FEA1
Activation Code
You may leave the Activation Code field empty and register your product later.
Up to 30 days from the first installation date of GuardNVR is available for evaluation.
InstallShield
< Back
Next >
Cancel

Activation Screen

You are able to enter the activation code during the installation, during the first GuardNVR launch or even afterwards.

To get your Activation Code contact the Quadrox sales department.

Store your activation code somewhere or write it on a label stuck on the inside of your Server. This code always stays the same and is needed again if reinstallation of the GuardNVR software is required.

13. Select **Restart the computer now** and click **Finish**.

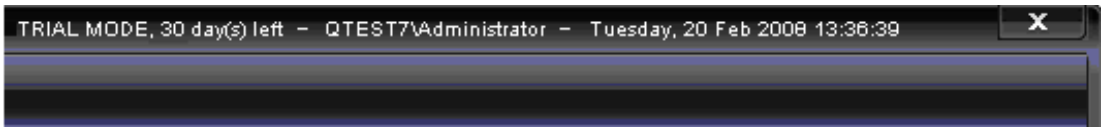
2.3.1 Trial mode

You are able to use GuardNVR in trial mode. To do so click **Continue Trial** during the launch of the GuardNVR web application in the Activation screen.

Activation Screen

Trial mode is valid during 30 days starting from the initial installation. After 30 days you won't be able to use GuardNVR and need to activate the software. Contact the Quadrox sales department to get an activation code.

You can see the remaining trial days in the right top corner of the GuardNVR web application.



To activate or upgrade your GuardNVR server, go to **Video Manager -> Info** and click **Update**. Enter your activation code in the window that appears and confirm.

You can activate your GuardNVR server during installation, in trial mode at start up of the GuardNVR web application or afterwards as described above.

2.4 Starting up for the first time

This chapter provides information on the following topics:

- Desktop icons overview
- Loggin on to GuardNVR server
- Changing password
- Setting time
- Changing keyboard settings
- Adjust screen resolution

2.4.1 Desktop icons overview

GuardNVR Server's Desktop

The following shortcuts should appear on your desktop after GuardNVR installation

Start Video Server. By double-clicking this icon, the user can start the GuardNVR's video server. If the video server is already started, double-clicking doesn't change anything.

Stop Video Server. By double-clicking this icon, the user can stop the GuardNVR's video server. If the video server is already stopped, double-clicking doesn't change anything.

Video Browser. By double-clicking this icon, the user starts the GuardNVR web application on the local GuardNVR video server.

Video manager. By double-clicking this icon, the user starts the GuardNVR web application on the local GuardNVR video server. The system can be managed and configured here.

Local Application. By clicking on this icon in the system tray, the user can access the GuardNVR local application.

2.4.2 Logging on to GuardNVR server

GuardNVR software uses the Windows Authentication system. Since the Windows main administrator is an administrator of GuardNVR, you are able to log on under its credentials.

If you're logged on to Windows with an account that is also registered as user in GuardNVR, you will be logged on automatically when opening the web application.

To create GuardNVR users, see chapter **3.2 Users** of the User manual.

2.4.3 Changing password

To change the Administrative password, follow the steps below:

- Go to **Start -> Control Panel**.
- When in Control Panel, select **User Accounts** from the right-hand list.
- In the User Accounts screen, select the **Administrator** user.
- Click Change my password link.
- Enter your current password.

The default Administrator password is webcctvnvr.

The default Administrator password is **webcctvnvr**. If you have an 'AZERTY' keyboard, it becomes **zebcctvnvr**. See **Chapter 2.4.5** how to change this to Azerty settings.

- Enter a new password and confirm it.
- Click Change Password button to save new Administrator account password.

When you change the Administrator password in Windows, the Administrator password of the GuardNVR application is automatically changed to this password. This means also that when you change your password in the GuardNVR application, that your Windows password will be changed automatically!

2.4.4 Setting time

For proper functioning of GuardNVR, it is very important to use the appropriate Time Zone setting because the movie recordings are always stored in local time This can be done in two ways, or by the **GuardNVR application configuration** (See **GuardNVR User Manual Chapter 3.3.10 Time Synchronisation**), or by the **Windows OS configuration**.

We strongly advise you to use the GuardNVR application way as this is the easiest way to configure your time settings.

2.4.4.1 Through GuardNVR Web Application

Time synchronization allows you to synchronize time on all devices connected to your unit (e.g. cameras) and synchronize your server with a specific time server. This can be done by going to the **Settings** menu in the **Video Manager** Web Application and selecting the **Time Synchronisation** link in the top bar

Time Synchronization Screen

There are three options:

- **Use video server as a (proxy) time server** – The unit will synchronize with an external time server if configured in the bottom part of the screen. If empty, the unit will act as a time server for itself and the connected devices (e.g. cameras).
- **Synchronize all devices with an external time server** – The unit and all the connected devices (e.g. cameras) will be synchronized with an external time server. Configure the IP address or DNS name of the external time server in the bottom part of the screen.
- **Manually configure time synchronization on each device separately (not recommended)** – No synchronization at all is performed, neither for the unit nor for the connected devices (e.g. cameras)

If your unit is part of a domain, this menu will not be available. The unit and connected devices (e.g. cameras) will be synchronized automatically with the Active Directory of the domain.

Click **Apply** to save the settings.

2.4.4.2 Through Operating System (XP or Vista)

2.4.4.2.1 Changing time zone

To change the time zone, follow the steps below:

- In **Control Panel**, in the left upper corner click the link 'Switch to Classic view'.
- When in classic view, select **Date & Time** from the right-hand list.
- On the Date and Time properties dialog, select the tab '**Time Zone**' (XP) or click '**Change Time Zone**' (Vista)
- When in the '**Time Zone**' menu, select the correct time zone.
- Click **OK** to save the 'Date and Time' changes.

To adjust the Date and time manually follow the steps below:

- In the **Control Panel**, in the left upper corner click the 'Switch to Classic view' link.
- When in classic view, select **Date and Time** from the right-hand list.
- On the **Date and Time properties** dialog, select the '**Date & Time**' tab (XP) or click '**Change Date & Time**' (Vista).
- When in the '**Date & Time**' menu, set the correct date and time.
- Click **OK** to save the 'Date and Time' changes.

2.4.4.2.2 Time synchronization

Synchronize your computer time with the atomic clock on the Internet for the best time accuracy.

Optionally the installer/user can configure a GuardNVR to synchronize its time and date automatically on a regular basis using a so-called 'Time Server'. These special servers exist often on bigger corporate networks or on the Internet. To set this up, follow the steps below:

- Click **Settings -> Control panel**.
- In **Control Panel**, in the left upper corner click the 'Switch to Classic view' link.
- When in classic view, select **Date and Time** from the right-hand list.
- On the Date and Time properties dialog, select the tab '**Internet Time**' (XP) or click '**Change Settings**' (Vista).
- Check the box '**Synchronize with an Internet time server**'.
- Enter the **name or IP-address** of a known time server into the 'Server' edit box. Note that when using a name in the IP-address settings of the GuardNVR server, a correct DNS IP-address should be supplied. Otherwise this name will never be resolved/found. If you use an IP-address there is no need to provide a DNS server.
- Click **OK** to save the 'Internet Time' changes.

The default Internet Time Server is time.windows.com; however you can use other time servers for synchronization, such as those provided below:

- time.nist.gov (IP-address: 192.43.244.18)
- utcnist.colorado.edu (IP-address: 128.138.140.44)

Make sure that there is no computer in the network with the same IP address.

2.4.5 Changing keyboard settings

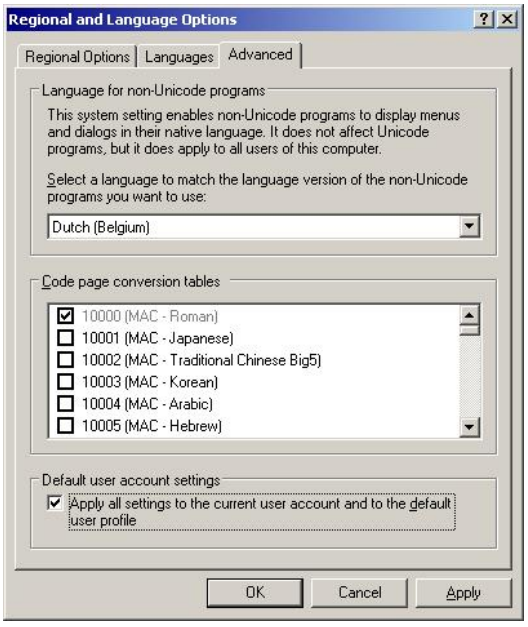
Follow the steps below:

- In **Control Panel**, in the left upper corner click the link 'Switch to Classic view'.
- When in classic view, select **Regional and Language Options** from the right-hand list.
- In the **Regional and Language Options** dialog, select the '**Languages**' tab.
- When on the '**Languages**' tab, click the '**Details**' button. The following window appears:

Keyboard Settings Screen

- In the **Text services and Input languages** dialog, add the desired keyboard layout.
- After adding the new keyboard layout, delete the other keyboard layouts.
- Use the 'Default Input Language' combo box to select the keyboard layout you added.
- Click **OK** to change the keyboard layout.
- In the **Regional and Language Options** dialog, select the '**Advanced**' tab.
- Select your **language** in the upper list box and enable the check box for **Default user account settings**. Click **OK** or **Yes** for all pop ups.

Changing keyboard settings on Vista is almost the same. Please check your OS manual for more information if necessary.


Regional and Language Options
Regional Options
Languages
Advanced
Language for non-Unicode programs
This system setting enables non-Unicode programs to display menus and dialogs in their native language. It does not affect Unicode programs, but it does apply to all users of this computer.
Select a language to match the language version of the non-Unicode programs you want to use:
Dutch (Belgium)
Code page conversion tables
10000 (MAC - Roman)
10001 (MAC - Japanese)
10002 (MAC - Traditional Chinese Big5)
10003 (MAC - Korean)
10004 (MAC - Arabic)
10005 (MAC - Hebrew)
Default user account settings
Apply all settings to the current user account and to the default user profile
OK
Cancel
Apply

Change Default User Settings
You chose to apply these settings to the default user profile.
These changes will affect the logon screen and all new user accounts. Some system services may require you to restart your computer before the changes will take effect.
OK

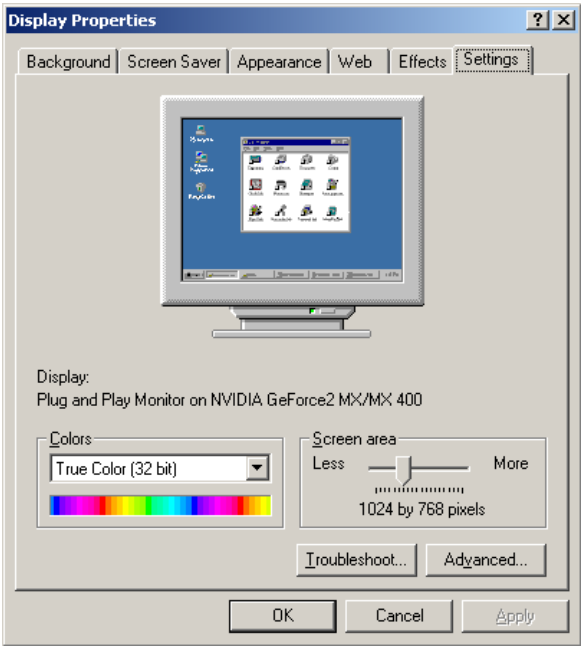
Advanced
The required files are already installed on your hard disk. Setup can use these existing files, or Setup can recopy them from your original Windows CD-ROM or from a network share.
Would you like to skip file copying and use the existing files? (If you click No, you will be prompted to insert your Windows CD-ROM or to supply an alternate location where the needed files may be found.)
Yes
No

- Click **OK** to save the 'Regional and Language Options' changes.

2.4.6 Adjusting screen resolution

To adjust the screen resolution, follow the steps below:

- Click **Start-> Settings-> Control panel-> Display**.
- On the **Settings** tab, under **Screen resolution**, drag the slider, and then click **Apply**.
- When prompted to apply the settings, click **OK**. Your screen will turn black for a moment.
- Once your screen resolution changes, you have 15 seconds to confirm the change. Click **Yes** to confirm the change; click **No** or do nothing to revert to your previous setting.



Display Properties Screen

A higher screen resolution reduces the size of the items on your screen and increases the relative space on your desktop.

Your monitor and video adapter determine how high you can change your screen resolution. You may not be able to increase the resolution beyond a certain point.

Changes to screen resolution affect all users that log on to the computer.

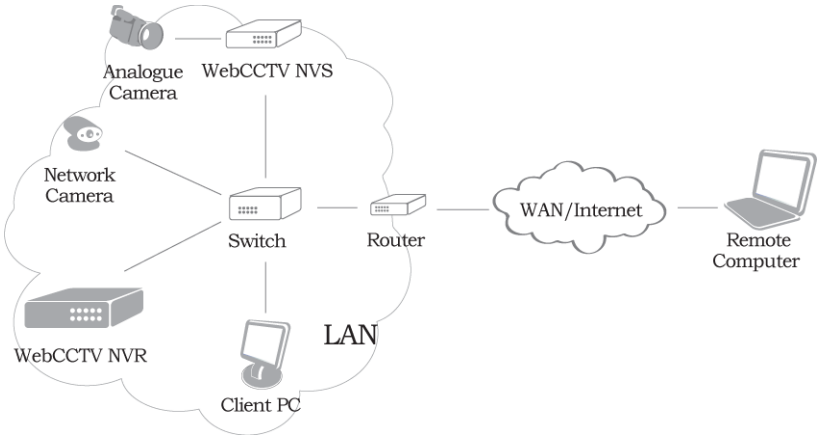
Only the recommended screen resolutions are listed. For additional settings, click the **Advanced** button on the **Settings** tab, click the **Adapter** tab, and then click **List all Modes**. Select the resolution, colour level, and refresh rate you want.

For Vista users, please check the OS manual. The configuration differs slightly but the idea behind the configuration stays the same.

2.5 GuardNVR in the network

2.5.1 Network overview

This chapter gives the schematic representation of the network camera and WebCCTV NVS connections. To connect your network camera and NVS properly look at the following figure:



Connecting Network Camera and WebCCTV NVS Scheme Screen

To configure your network camera, please refer to the manufacturer's manual supplied with the network camera.

To add a network camera to GuardNVR (WebCCTV NVR in this scheme), refer to the Camera Wizard chapter in the User manual.

Please note that a list of all supported cameras may be found in **Appendix C**.

Analogue cameras can also be connected directly to the GuardNVR when a digitizer card is present on the GuardNVR.

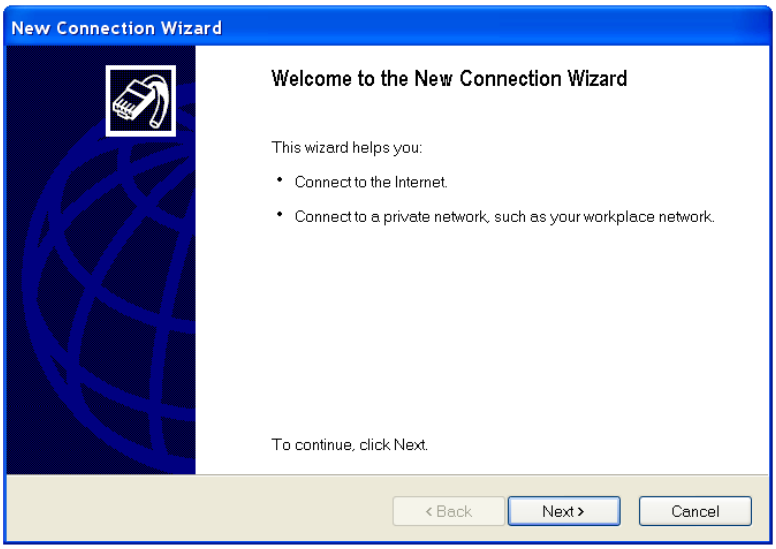
2.5.2 Connecting GuardNVR to the local network

When you start your GuardNVR system, your operating system detects your network adapter and automatically starts the local area connection. Unlike other types of connections, the local area connection is created automatically, and you do not have to click the local area connection in order to start.

A local area connection is the only type of connection that is automatically created and activated.

To establish connections of another type follow the steps below:

1. Click **Start -> Settings** -> **Control panel** -> **Network connections**
2. In the Network connections window click **File**-> **New connection**. You'll see the following window:


New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
To continue, click Next.
< Back
Next >
Cancel

Network Connection Wizard Screen

Follow the prompts the network connection wizard provides to define your unit in the network.

For obtaining more detailed information about your network settings, please contact your system administrator or check the OS manual.

2.5.3 Assigning IP address

If you cannot use DHCP or APIPA for IP address and subnet assignment, the IP address for the Windows OS-based client must be manually configured. The required values include the following:

- An IP address for each network adapter installed on the computer.
- The Subnet mask corresponding to each network adapter's local network.

In order to facilitate remote connections to GuardNVR, it is recommended you use a **static IP-address**.

To manually configure an IP address on Windows XP, follow the steps below:

- Click **Start->Settings->Control Panel**.
- In Control Panel, select **Network and Internet Connections**.
- On the Network and Internet Connections sheet, select **Network Connections**.
- In Network Connections, **right-click the local area connection** that you want to modify.
- Select **Properties**.
- On the General tab of the Properties sheet, select **Internet Protocol (TCP/IP).**
- Click **Properties**.
- On the General tab of the TCP/IP Properties sheet, select the **Use the following IP address** option.
- Enter the **IP address**, **subnet mask**, and **default gateway** for the selected adapter in their respective text boxes. The network administrator must provide these values for individual users, based on the IP addressing scheme for your site. The value in the IP Address text box identifies the IP address for this network adapter. The value in the Subnet Mask text box is used to identify the network ID for the selected network adapter. If needed, the **DNS server address** can be entered also.
- Click **OK** to save the IP addressing information.
- Click **OK** to save the connection properties.

For Vista users, please check the OS manual. The configuration differs slightly but the idea behind the configuration stays the same.

2.5.4 Firewall configuration

The following ports need to be opened for connections going **towards** the GuardNVR:

1. **TCP** Port 80: http
2. **TCP** Port 1518: GuardNVR control connection
3. **UDP** Ports 4096 till 4223: GuardNVR video streaming
4. **TCP** Port 3389: Remote Desktop connection **(Optional)**. Frequently asked by support when you have an issue)

RTP uses two UDP ports per stream (versus one in the old streaming format in versions prior to V4.0.0.0), one for RTP (the video stream itself) and one for RTCP (QoS signal stream), limiting the software to a maximum of 64 concurrent streams. This number can be limited (e.g. for security purposes) or extended using the **Settings > Network settings** page. In that case, Quadrox recommends you to open a number of spare ports to avoid switching issues, e.g. 4 ports extra. The first port in the range should be even.

Like all applications which communicate over networks, GuardNVR uses communication channels to pass data (commands, video, web-pages, etc …) back and forth. **The network language that the GuardNVR uses is called TCP/IP.** This is not a unique language but a

family of related network languages, called network protocols. These TCP/IP protocols are the network protocols used on the Internet and on most networks throughout the world today. GuardNVR uses two protocols specifically: **TCP** and **UDP**.

A communication channel on a TCP/IP network can be represented as a tunnel with two endpoints. The two programs communicating with one another are each said to be at each endpoint. These endpoints are called **ports**.

When the two programs communicating with one another are not located on the same corporate network (like most communication between a program on a client PC and a program running on another computer on the Internet), often there is some kind of guardian device in between them. These guardian devices are called **Firewalls.** Their job is to guard all network communication between the corporate network and the Internet and block certain unwanted communications while allowing the desired communication to pass.

There are several levels on which a firewall can guard network communication. The most common way is to allow or disallow certain ports to be used, depending on which applications are allowed to communicate.

A firewall guards a port in a certain direction. Communication that is initiated from the Internet towards the corporate network is called incoming traffic, while communication from the corporate network towards the Internet is called outgoing traffic. Note that the *initiation* of the communication is important: once a connection is made, data can be transferred in both directions.

Let's apply this principle to GuardNVR network communication. The GuardNVR client (the ActiveX component embedded in Internet Explorer at the client machine) will try to create network connections to the GuardNVR server. The eventual result of these connections will be video data streaming from the GuardNVR server to the GuardNVR client, but since the GuardNVR client initiates them, they are referred to as connections towards the GuardNVR. From the client perspective, it is outgoing traffic, while for the server it is incoming traffic.

In order for the GuardNVR to function correctly, the appropriate ports need to be opened for communication **towards** the GuardNVR.

There are three port configurations to perform:

1. **TCP Port 80**: to allow external users to see the web interface (HTTP traffic). This port is usually opened by default.

Some ISPs block port 80. Please inform yourself.

2. **TCP Port 1518**: to allow external users to receive alarms, control PTZ cameras, send commands, etc. This is called the GuardNVR control signal.
3. **UDP Ports 4096 till 4223**: By default the GuardNVR uses a range of UDP ports to transport video streams. These UDP ports are not listening all the time. The GuardNVR software enables them at random to enhance security.

Typically when the UDP ports are not opened correctly, the user only sees the web-interface but no live images.

To allow Quadrox support personnel to get remote access to the GuardNVR, TCP Port 3389 needs to be opened for Remote Desktop Connection or 5500 for VNC.

A firewall can be placed on several positions in the network. The most common place is at the edge of the corporate network, or in other words between the corporate network and the Internet. Recently it also became popular to place a firewall to protect the network traffic from a single computer. A firewall that is placed between the computer and the network is referred to as a 'Personal Firewall' application.
In practice, a corporate network firewall is often integrated with the router connecting the LAN and the internet. For more information on routers, see the section on connecting the GuardNVR to the internet. A personal firewall is software running on the computer that it protects. Personal firewall applications can be installed separately but are also included in the Windows XP operating system (Service Pack 2) or Vista and in many virus protection software packages.

There are several scenarios where firewall configuration is necessary:

1. A user on a corporate network or at home behind a broadband router wants to access a GuardNVR on the Internet
2. A user on the Internet wants to access a GuardNVR on a corporate network.

These situations are explained in more detail in the section on how to connect your GuardNVR to the internet. If a user on a corporate network wants to connect to a GuardNVR on another network, a logical combination of these two situations can be applied.

1. A user with a personal firewall application on his computer wants to access a GuardNVR on the corporate network or on the Internet.
2. There is a personal firewall application installed on the GuardNVR.

2.5.5 Connecting a client

2.5.5.1 Minimum client requirements

Operating system

- Windows XP SP3
- Windows Vista
- Windows 7

64-bit Operating Systems are not yet supported.

Hardware

- Intel Dual Core or higher
- 1024 MB RAM
- 128 MB RAM on the video card

Software

- Internet Explorer 7 or higher
- DirectX 9.0c

Media players and codecs

- Windows Media Player 11
- Windows Media Formats 11

Some useful downloads are available in the **System Downloads** menu. See the User Manual for more information.

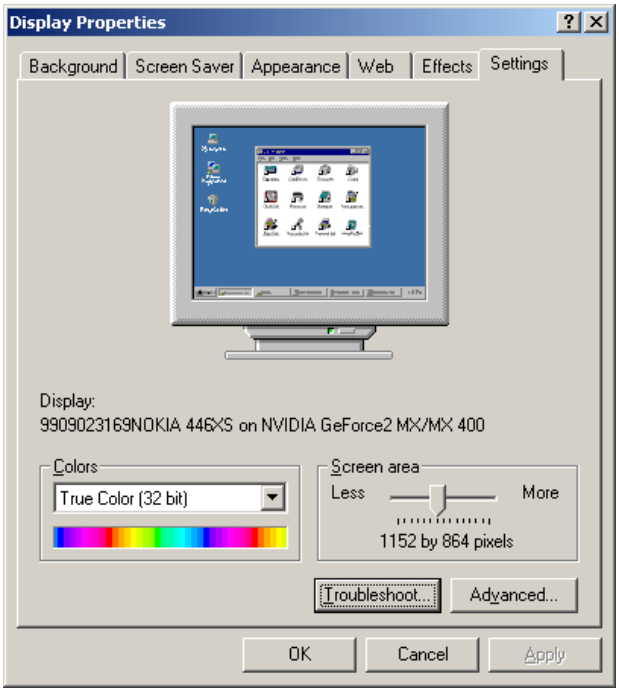
In case you are using WebCCTV Network Video Servers (NVS) or have IP cameras that stream in MPEG or H.264, a codec also needs to be installed. We advice you to install the **Quadrox Codec Pack** which can be found in the System Downloads menu (See User Manual for more information) or on the support pages of www.webcctv.com.

2.5.5.2 Client configuration

Hardware video acceleration

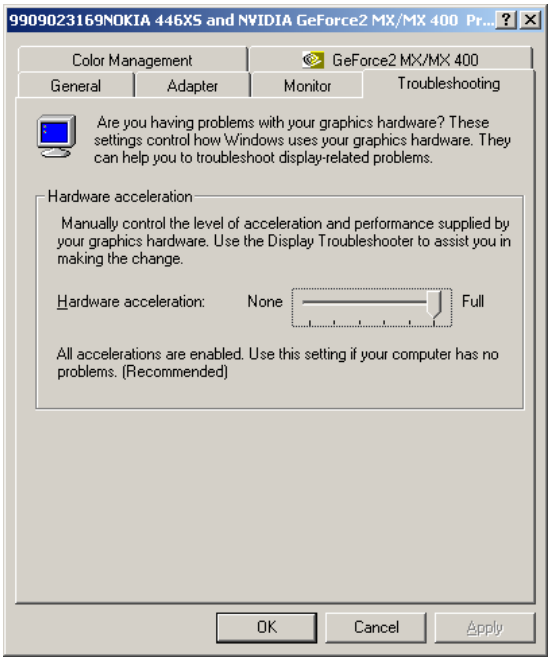
In order to enjoy all the features of GuardNVR, the hardware acceleration of your video card needs to be enabled.

1. Right click on the desktop and choose **properties**.
2. Select the **Settings** tab and click the **Advanced** button.



Display Properties Screen

3. Choose the **Troubleshooting** tab and put the hardware acceleration to **Full.**


9909023169NOKIA 446XS and NVIDIA GeForce2 MX/MX 400 Pr...
Color Management
GeForce2 MX/MX 400
General
Adapter
Monitor
Troubleshooting
Are you having problems with your graphics hardware? These settings control how Windows uses your graphics hardware. They can help you to troubleshoot display-related problems.
Hardware acceleration
Manually control the level of acceleration and performance supplied by your graphics hardware. Use the Display Troubleshooter to assist you in making the change.
Hardware acceleration:
None
Full
All accelerations are enabled. Use this setting if your computer has no problems. (Recommended)
OK
Cancel
Apply

Troubleshooting Tab Screen

Sometimes the support department will ask you to put this setting to None in order to customize your system for particular use scenarios.

Firewall

If you have a personal firewall, configure it according to chapter 2.5.4. The ports for outgoing connections should be opened.

A personal firewall is included in Windows XP Service Pack 2 or Vista and also in some virus scanners. Separate firewall software exists as well.

The personal firewall in Windows XP Service Pack 2 and Vista has all outgoing and necessary incoming connections open by default. No extra configuration is necessary in this case.

Internet Explorer settings

Make sure that Internet Explorer allows the installation and execution of signed ActiveX components.

1. Make sure you are logged on to Windows as an Administrator.
2. Go to the **Tools** Menu. Choose **Internet Options**.
3. Go to the **Security** Tab.
4. Click the **Sites** button, deselect the https checkbox and add your GuardNVR to the trusted sites list. Click **OK**.
5. Click the **Custom level** button at the bottom.
6. Set the following options to **'enable'** or **'prompt'**:
7. Download signed ActiveX controls (prompt)

8. Run ActiveX controls and plug-ins (enable)
9. Script ActiveX controls marked as safe (enable)

Adding your GuardNVR to the trusted sites is required to guarantee that all necessary communication can be established with the GuardNVR server!

Anti-virus and anti-spyware/malware software

Make sure that your anti-virus and anti-spyware/malware software is set to...

1. Allow the GuardNVR ActiveX component to install and execute. (See also Internet explorer settings)
2. Allow scripts to be executed.

The web application of the GuardNVR relies heavily on both issues.

2.5.6 Connecting GuardNVR to the Internet

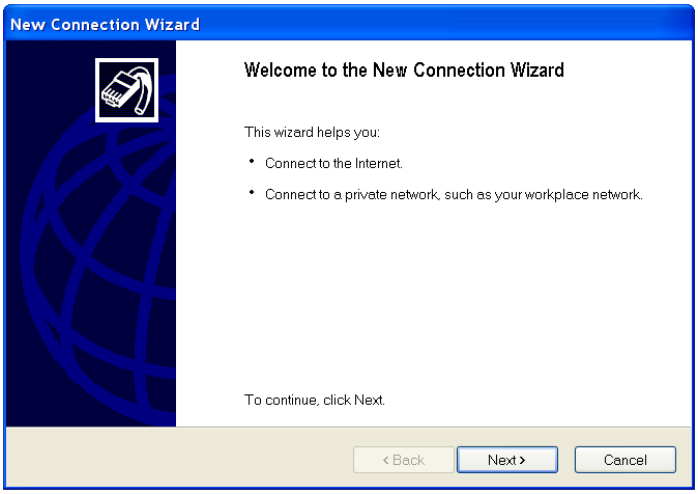
2.5.6.1 Creating a network connection

When you start your GuardNVR, Windows XP or Vista detects your network adapter and automatically starts the local area connection. Unlike other types of connections, the local area connection is created automatically, and you do not have to click the local area connection in order to start.

A local area connection is the only type of connection that is automatically created and activated.

To establish connections of another type follow the steps below:

- Click **Settings** -> **Control panel** -> **Network and Internet connections**
- In the Network and Internet connections window click **File**-> **New connection**. You'll see the following window:


New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
To continue, click Next.
< Back
Next >
Cancel

Network Connection Wizard Screen

Follow the prompts the Network connection wizard provides to define your unit in the network.

For obtaining more detailed information about your network settings please contact your system administrator or check the OS manual.

2.5.6.2 Router and firewall

To fully understand this section it is important to know what the difference between a router and a firewall is.

A **firewall** is the piece of software that takes care of guarding the network communications. Sometimes the term 'firewall' refers to the machine performing firewall tasks. This is confusing and in fact incorrect: normally a firewall is not a piece of hardware, but a program running on that hardware.

A **router** is a piece of hardware that embodies the physical connection between two different networks (e.g. your local network and the Internet). It redirects ("routes") data so that it arrives at the correct place. A router is a hardware device, but its functionality is controlled by software that runs on the router.

Sometimes the routing functionality is provided by a proxy server, bridge or gateway. While these are not the same as routers, they can be considered as such for the discussion in this document.

Router software can have firewall capabilities. In other words, the router software can have, apart from its normal capability to connect two networks and redirect data, the capabilities of inspecting, allowing, and denying certain network communication. As an example, most broadband routers (ADSL, SDSL, cable modems, etc) nowadays have firewall capabilities and are also being used as such.
In the following schemes the firewall and the router are depicted as two different entities (nodes on the network), but know that they could be one and the same node in practical cases.

2.5.6.2.1 Configuring router

The router that forms the connection between the corporate network and the Internet needs to know which internal machine it has to send network traffic to.
For example, a client machine on the internet requests a connection on port 1518 (the port for GuardNVR video commands), using the public IP address of the router. The router then needs to know to which device on the corporate network it needs to send this connection request, in this case the GuardNVR. So the router needs to know the local IP address on the corporate network of the GuardNVR. Configurations for different brands and models of routers in the field can be found in:

Web Resource for Router Configuration and Setup:
http://www.portforward.com/routers.htm

Networking Tips:
http://www.portforward.com/network.htm

If you don't already have a router you will need to purchase one and configure it as part of you network.

Useful commands

ipconfig – utility to see computer IP properties
ipconfig /release – release the current IP address – need DHCP enabled
ipconfig /renew – renew the IP address by telling the router that it needs DHCP enabled
ipconfig /all – show all IP config properties
ipconfig /? – show help on IP config

ping – utility to test the connection with other IP address
ping 192.168.123.254 – attempt to ping IP address by sending a small packet
ping –t 192.168.123.254 – continually ping IP address until you close command window or hit Ctrl+C.

DHCP – Dynamically assign IP address to requesting devices (e.g., computer, camera). This means when you connect a computer to the router the computer will automatically negotiate an IP address from the router.

Port Mapping – Section on router where you specify which port will be mapped to which device. With a router you are sharing a single Internet connection with multiple devices and for the cameras you need to have each camera on a separate port if you want to access the camera from outside the router (i.e., Internet).

2.5.6.2.2 Configuring firewall

General information about firewalls and their configuration is given in a previous section. The most important notes are:

The following ports need to be opened for connections going towards the GuardNVR:

1. **TCP** Port 80: http
2. **TCP** Port 1518: GuardNVR control connection
3. **UDP** Ports 4096 till 4223: GuardNVR video streaming

In order for the GuardNVR to function correctly, the appropriate ports need to be opened for communication **towards** the GuardNVR.

The following port needs to be opened for connections going **outwards** from the GuardNVR:

1. **TCP** Port 3389: Remote Desktop Connection port. This port is used in support cases only.

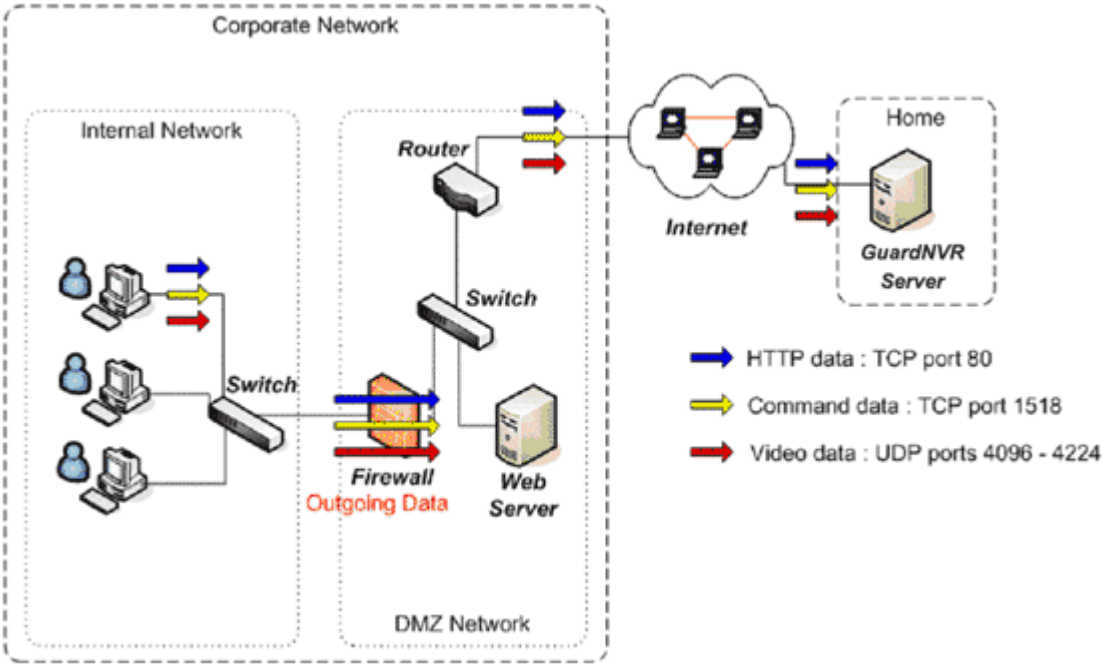
RTP uses two UDP ports per stream (versus one in the old streaming format), one for RTP (the video stream itself) and one for RTCP (QoS signal stream), limiting the software to a maximum of 64 concurrent streams. This number can be limited (e.g. for

security purposes) or extended using the **Settings > Network settings** page. In that case, Quadrox advises to open a number of spare ports to avoid switching issues, e.g. 4 ports extra. The first port in the range should be even.

Let's apply this to the two situations in which a GuardNVR is accessed over the Internet.

The blue, yellow and red arrows in the following diagrams indicate the direction of the initial network connection request, and thus the direction in which the ports should be opened in the firewall.

Situation 1 – A user on a corporate network or at home behind a broadband router wants to access a GuardNVR on the Internet

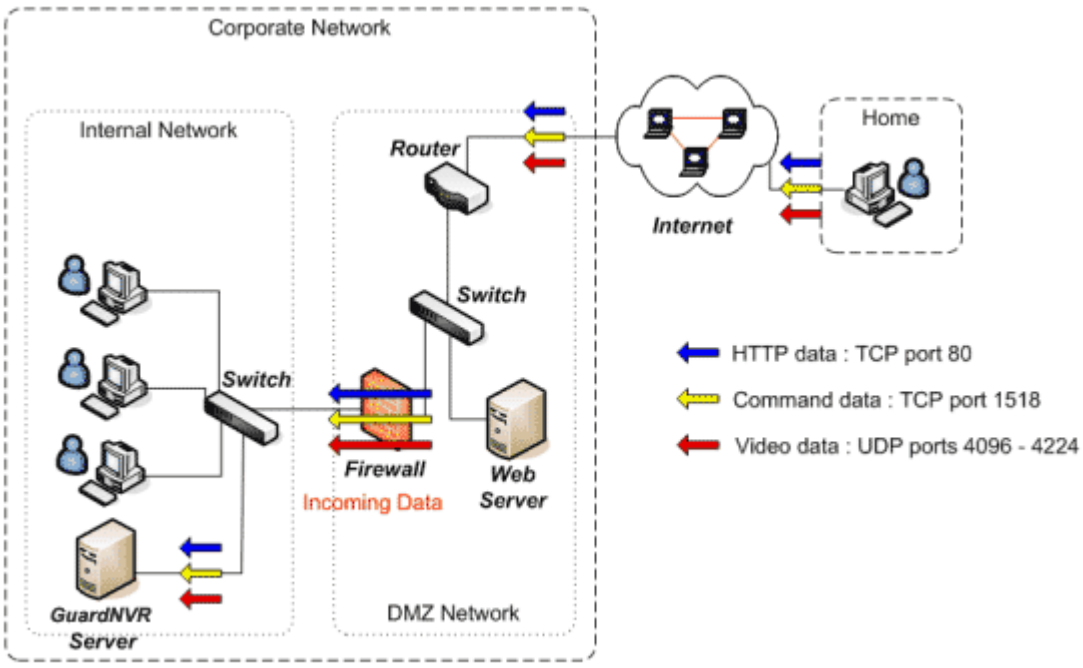


The user on a corporate network wants to access GuardNVR over the Internet. The main concern is: will the corporate firewall allow the GuardNVR network traffic?

The client computer makes the initial connection to the GuardNVR server. The firewall should allow data going out of the corporate network to the GuardNVR. The appropriate ports should thus be opened for outgoing data.

Note that not all of the UDP ports are used all the time. However, since the GuardNVR software assigns them randomly, the exact ports cannot be known beforehand. The network administrator should open the full range of UDP ports.

Situation 2 – A user on the Internet wants to access a GuardNVR on a corporate network



The user is connected to the internet and wants to access a GuardNVR, which is located on a corporate LAN (Local Area Network). The main concern is: will the corporate firewall allow the incoming GuardNVR network traffic?

The client computer makes the initial connection to the GuardNVR server. The firewall should allow data coming in to the corporate network to the GuardNVR. The appropriate ports should thus be opened for incoming data.

2.6 Testing GuardNVR

2.6.1 Local client test

A local client test is very useful, to test whether the video server is running correctly on its own. Because we don't use any external network facility, no configuration in that direction can cause a live-viewing problem. Perform this test first of all to check the stand-alone operation of the GuardNVR video server.

For local client testing, follow the steps below.

1. On the desktop of a GuardNVR, you'll find an icon 'Video Browser'. Double-clicking this icon will open a Microsoft Internet Explorer window.
2. The IP address (e.g.: http://192.168.100.1) to where this Internet Explorer has to connect looks like 'http://localhost/guardnvr/browser'. This is a standard way of telling Internet Explorer to connect to the webserver on the same GuardNVR, so not going over the network but staying within the boundaries of its own Operating System.
3. When accessing the GuardNVR video server application from a client PC for the first time, Internet Explorer will ask you to install and run an ActiveX component (Video Client Component). Follow the on screen instructions to install the component.

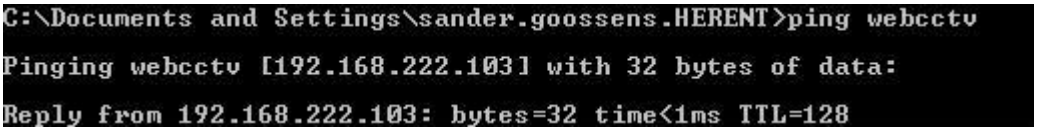
If you have problems installing the ActiveX, please make sure first that you have added the server to the trusted site list of Internet Explorer.

4. A welcome screen should now appear. Normally you would be prompted for a login and password but because you've already authenticated to get access to the Windows Operating System, and you will not be prompted again for a Login and Password.
5. By default the live-view pages are opened and the user can verify whether all the cameras are transmitting a good image.

2.6.2 Connection test

Open a command prompt window by clicking **Start**, select **Run**, and type **CMD**. Once the MS DOS window is open, type **ping <Computer Name>**.

- If you see the text **'Reply from XXX.XXX.XXX.XXX'** (as shown in Picture A), the network connection is fine.
- If you see the text **'Ping request could not find host <Computer Name>. Please check the name and try again.',** there is a physical network connection problem. Contact your Network Administrator.
- If you see the text **'Request Timed Out**', there is a physical network connection problem. Contact your Network Administrator.
- If you see the text **'Destination host unreachable'**, the IP address settings of either the client computer or the GuardNVR, is inconsistent (different subnets). Contact your Network Administrator.


C:\Documents and Settings\sander.goossens.HERENT>ping webcctv
Pinging webcctv [192.168.222.103] with 32 bytes of data:
Reply from 192.168.222.103: bytes=32 time<1ms TTL=128

Checking Physical Connection Screen

2.6.3 Remote client test

For remote client testing, follow the steps below:

1. Open a Microsoft Internet Explorer window.
2. Fill in the IP address (e.g.: http://192.168.100.1/guardnvr) or domain name (e.g.: http://guardnvr.mycompany.com/guardnvr) in the address bar.
3. When accessing the GuardNVR from a specific client computer for the first time, Internet Explorer will ask you to install and run an ActiveX component (Video Viewer Component). Follow the on screen instructions to install the component.

If you have problems installing the ActiveX, please make sure first that you have added the server to the trusted site list of Internet Explorer.

4. A welcome screen should now appear, and you will be prompted for a Login and Password.

After filling in Logon and Password you should be logged on to the GuardNVR Web Application.

'http://192.168.100.1/guardnvr' is the factory default IP-address for the EU version of GuardNVR. For US customers the factory default IP-address is **http://192.168.0.199/guardnvr.** Please note that your installer could have changed it to fit the specifications of your own network.

3 Upgrading & Restoring GuardNVR

3.1 Upgrading GuardNVR software

The GuardNVR software (and related installed components: Alarm, POS…) can be upgraded at all times when a new version is available and this without losing your settings and recordings. This is done by the the **ProductUpdate** tool and works for version 4.0.4.0 and higher. The ProductUpdate is a standalone InstallShield-based application that updates the currently installed GuardNVR application to the most recent version.

You can request this tool for free by contacting support@quadrox.com.

3.2 Saving and Restoring configuration

It is advisable to save the settings after the configuration process on a save place or medium such as a blank CD/DVD. When performing an upgrade or a complete system restore, you can use this configuration file to restore the GuardNVR configuration quickly and easily. You can restore any version starting from version 4.0.4.0.

To save or restore configuration settings, please read the **User Manual**.

4 Advanced topics

4.1 Extending storage space

You are able to add new hard disks to your GuardNVR server to increase movie storage capacity (this both inside or ouside the GuardNVR unit case). The following two sections describe how to first physically and after that logically add new storage space. The example focuses on adding one extra hard disk inside a GuardNVR Ser ver with an Windows XP OS. Other configurations are similar.

4.1.1 Adding hard disk

In order to add a hard disk to the GuardNVR, follow the steps below:

1. Make sure the GuardNVR is turned off completely by removing the power cable from the power supply at the back of the GuardNVR.
2. Remove the top cover.
3. Place the additional hard disk near the old one in the special tray.
4. Connect one side of a flat IDE cable to the second hard disk and the other side to the second IDE slot on the motherboard. In case of SATA, the procedure is similar.
5. Connect power cable to the hard disk.
6. Check the proper setting of the hard disk jumper. Both hard disks have to be configured as master when connected to two different IDE cables. If they are connected to the same IDE slot the main hard disk is a **Master**, the additional hard disk should be **Slave**. Please set the jumper to the **Slave** position. This step can be skipped if you use SATA.

To correctly configure the jumper settings, please visit the web site of the respective Hard Disk manufacturer:

HITACHI: www.ghst.com
MAXTOR: www.maxtor.com
SAMSUNG: www.samsung.com
SEAGATE: www.seagate.com
WESTERN DIGITAL: www.westerndigital.com

7. Close the top cover.
8. Turn on the power of the GuardNVR and make sure that the message that a new hard disk drive is detected appears. Normally you will be asked to save the new settings.

4.1.2 Configuring added hard disk

Adding a hard disk to the Windows Operating System can be done in multiple ways. We will discuss the two most used scenarios when speaking about GuardNVR:

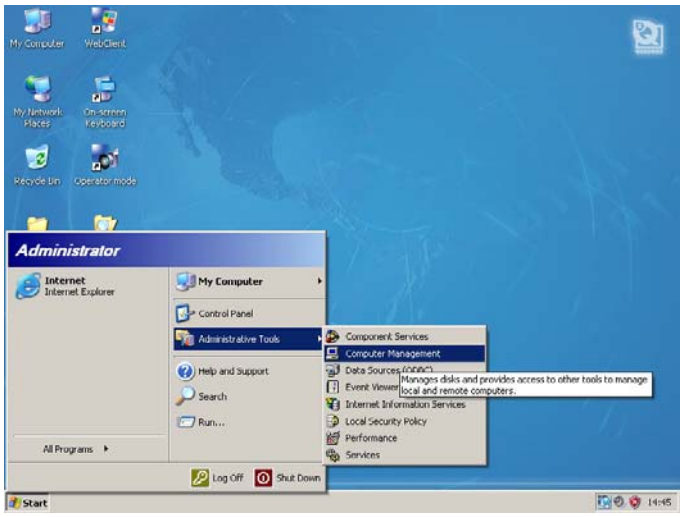
- **Single Disk Extension**: Two or more disks are merged to one disk for the Operating System.
- **Multiple Logical Disks**: Every hard disk is recognized as a separate disk on the Operating System.

The table below gives an overview of some advantages and disadvantages for each scenario. It's up to you to decide which scenario fits your needs the best.

	Single Disk Extension	Multiple Logical Disks
Optimized recording space	Yes	No
Optimized recording performance	No	Yes
Video Manager configuration	Practically none	Add volumes in storage manager menu
Installation procedure on Operating System	Hard	Easy

In order to configure the Windows Operating System to add more storage for recordings, follow the steps below:

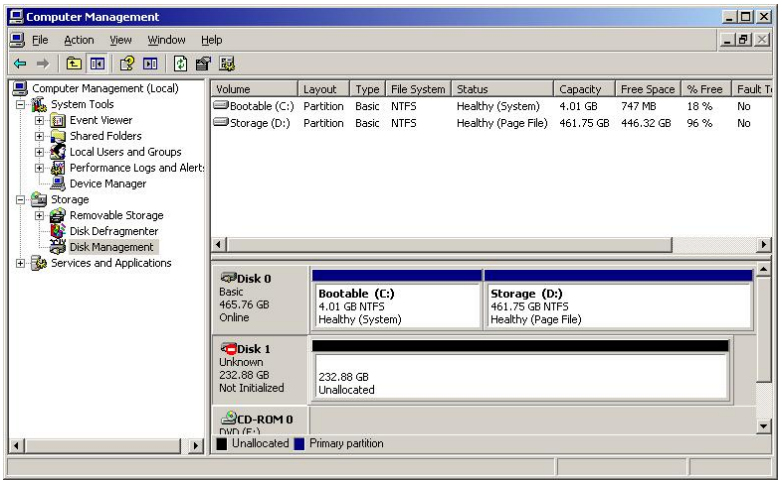
1. Make sure you followed all steps described in 4.1.1.
2. Logon as **'Administrator'** at the logon screen, so eventually you'll be in Administrative mode.
3. Go to **Start->Administrative Tools->Computer Management.**



Administrative Tools Menu Screen

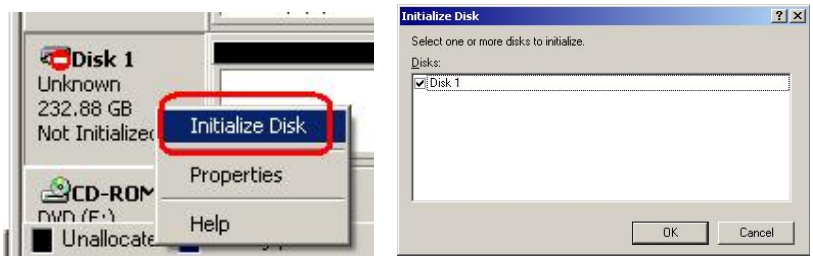
4. On the **Computer Management** window, select **Disk Management** in the left pane. In the right pane, you see the original disk **Disk 0** with 2 partitions, **Bootable** and **Storage**

and the new disk **Disk 1** which is Unallocated and still Unknown. In case the disk is not yet initialized (see screenshot), initialize the disk by clicking right on Disk 1 and selecting Initi.

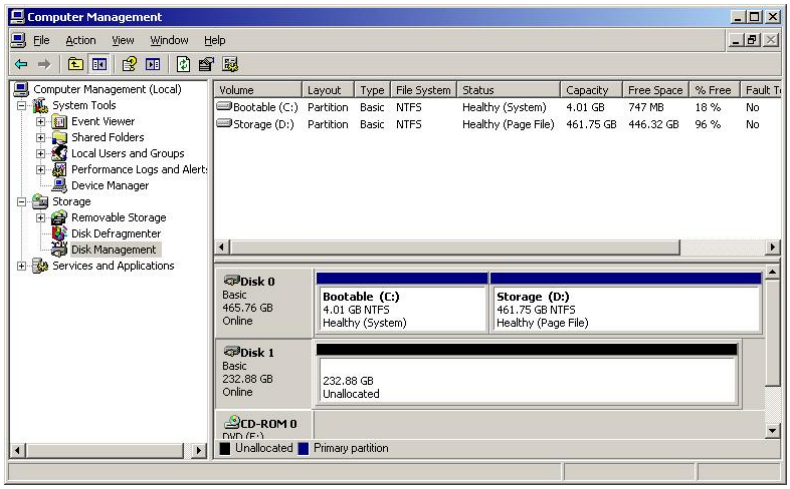


Computer Management Screen

5. In case the disk is not yet initialized (see screenshot above), initialize the disk by clicking right on **Disk 1** and selecting **Initialize Disk**.



6. Your screen looks now similar to the following screen.



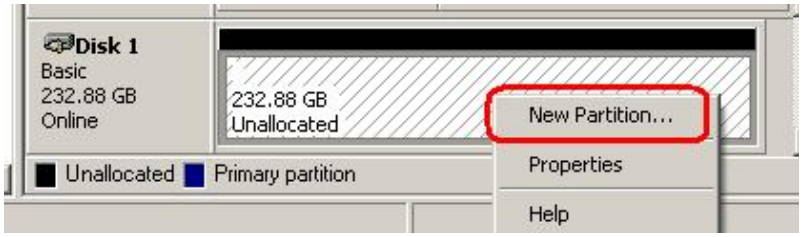
If you want to add your hard disk as:

a. Separate Logical Disk → Go to chapter **4.1.2.1 Multiple Logical Disks**
b. Extended Disk → Go to chapter **4.1.2.2 Single Disk extension**

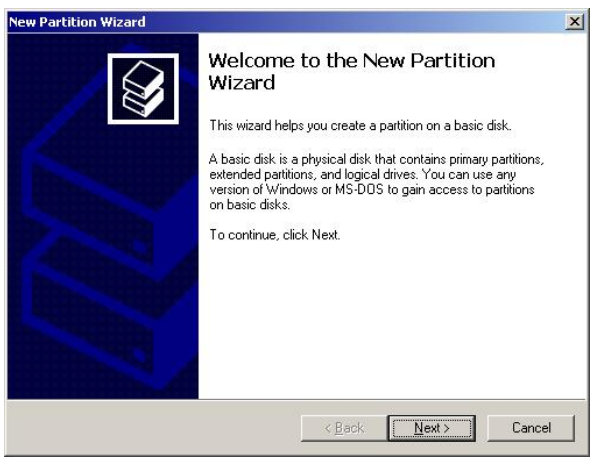
4.1.2.1 Multiple Logical Disks

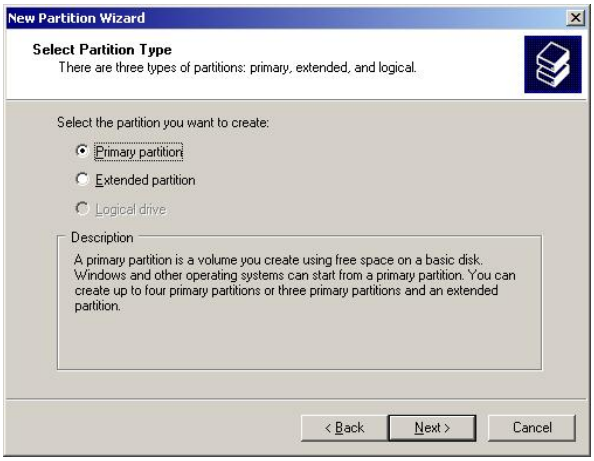
Before proceeding, make sure you followed all steps from chapter **4.1.2 Configuring added hard disk.** Please follow now the steps below:

1. Right click on the unallocated section and select **New Partition…**

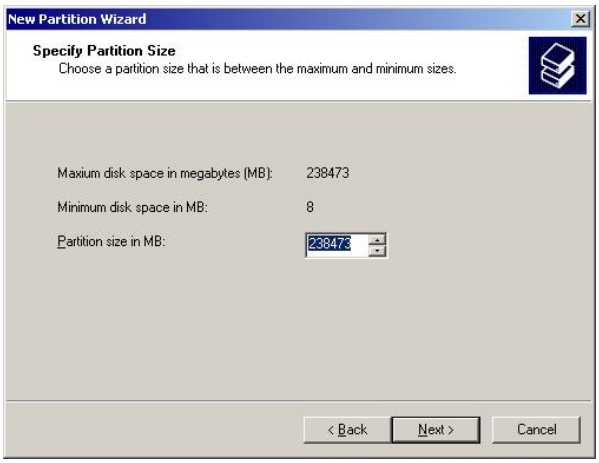


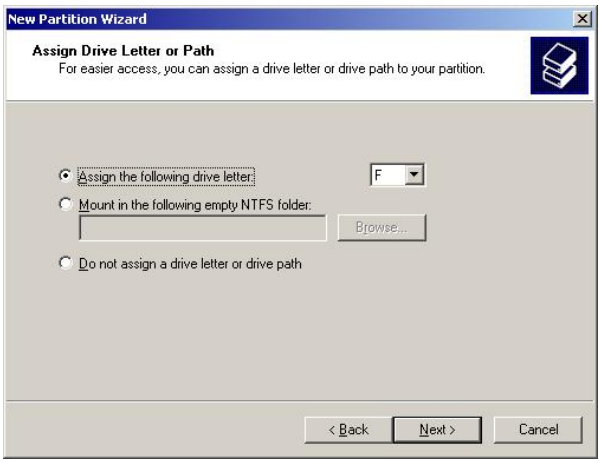
2. Follow the wizard and select **Primary partition**.


New Partition Wizard
Welcome to the New Partition Wizard
This wizard helps you create a partition on a basic disk.
A basic disk is a physical disk that contains primary partitions, extended partitions, and logical drives. You can use any version of Windows or MS-DOS to gain access to partitions on basic disks.
To continue, click Next.
< Back
Next >
Cancel

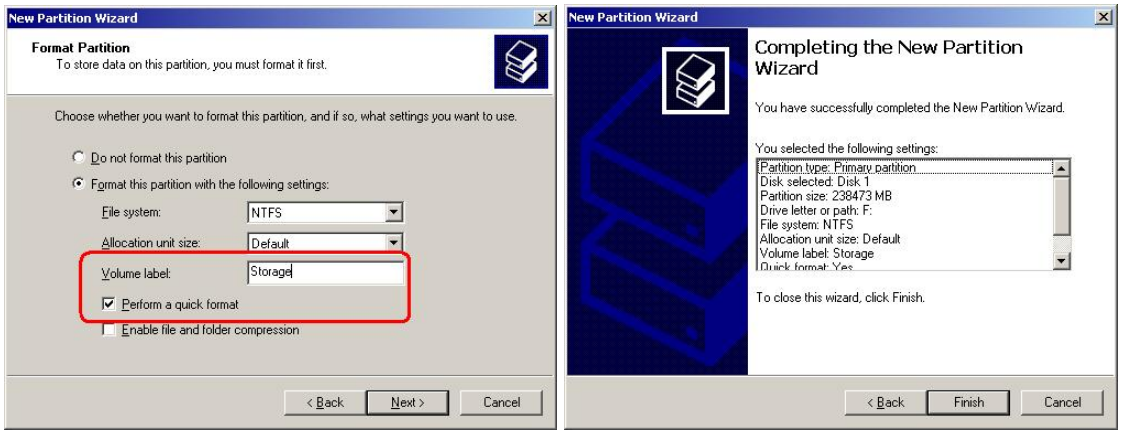

New Partition Wizard
Select Partition Type
There are three types of partitions: primary, extended, and logical.
Select the partition you want to create:
Primary partition
Extended partition
Logical drive
Description
A primary partition is a volume you create using free space on a basic disk. Windows and other operating systems can start from a primary partition. You can create up to four primary partitions or three primary partitions and an extended partition.
< Back
Next >
Cancel

3. Choose the partition size (by default it takes all available space) and assign a drive letter.

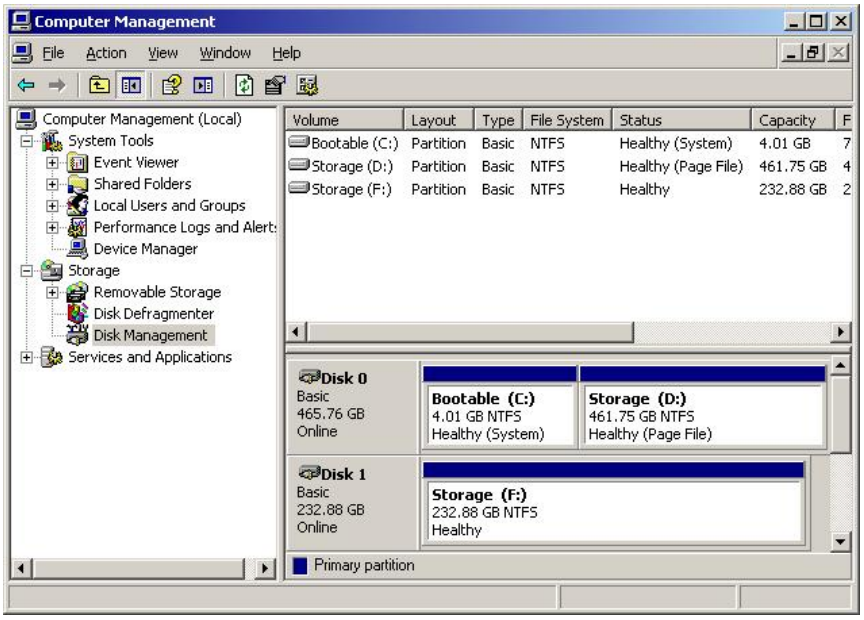

New Partition Wizard
Specify Partition Size
Choose a partition size that is between the maximum and minimum sizes.
Maxium disk space in megabytes (MB): 238473
Minimum disk space in MB: 8
Partition size in MB: 238473
< Back
Next >
Cancel


New Partition Wizard
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.
Assign the following drive letter: F
Mount in the following empty NTFS folder:
Browse...
Do not assign a drive letter or drive path
< Back
Next >
Cancel

4. Select **Perform a quick format** and assign a **Volume Label**. Then click **Finish**.


New Partition Wizard
Format Partition
To store data on this partition, you must format it first.
Choose whether you want to format this partition, and if so, what settings you want to use.
Do not format this partition
Format this partition with the following settings:
File system: NTFS
Allocation unit size: Default
Volume label: Storage
Perform a quick format
Enable file and folder compression
< Back
Next >
Cancel
New Partition Wizard
Completing the New Partition Wizard
You have successfully completed the New Partition Wizard.
You selected the following settings:
Partition type: Primary partition
Disk selected: Disk 1
Partition size: 238473 MB
Drive letter or path: F:
File system: NTFS
Allocation unit size: Default
Volume label: Storage
To close this wizard, click Finish.
< Back
Finish
Cancel

Your hard disk was added. If everything went fine, you will see a screen similar to the one below.

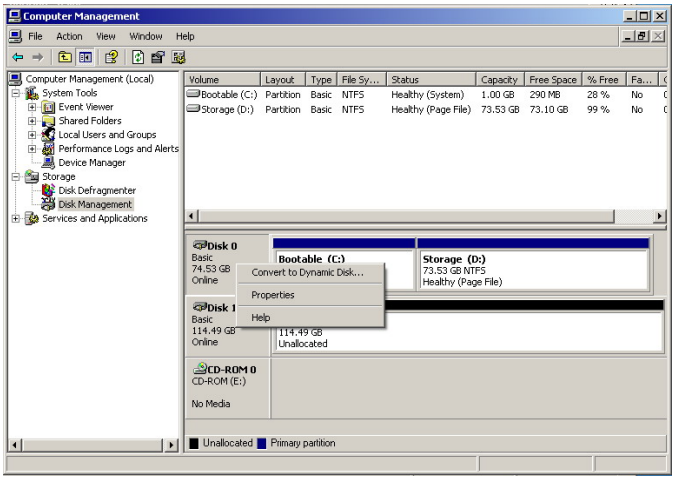


To add this new volume in the WebCCTV application, check **3.3.4 Storage Manager** in the **User Manual**.

4.1.2.2 Single Disk Extension

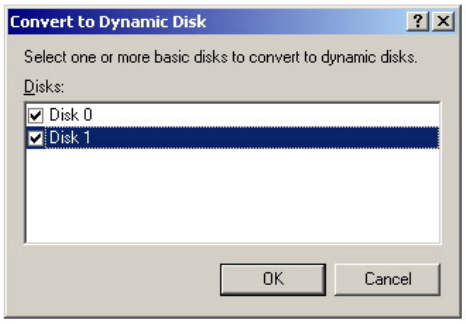
Before proceeding, make sure you followed all steps from chapter **4.1.2 Configuring added hard disk**. Please follow now the steps below:

1. Right-click **Disk 0** and select **'Convert to Dynamic Disk …'** from the popup menu.



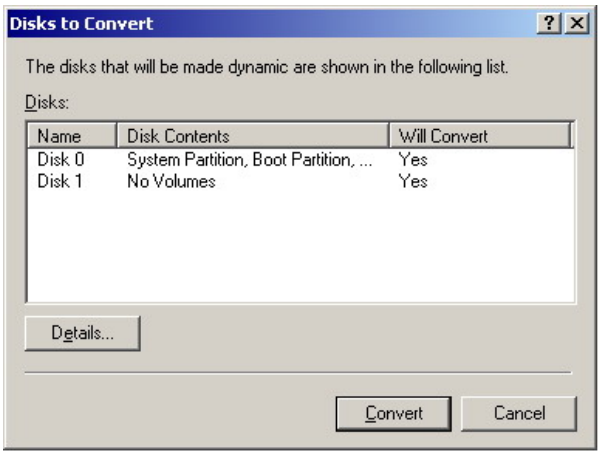
Computer Management Screen

2. In the **Convert to Dynamic Disk** window, select both disks to be converted. Click **OK**.



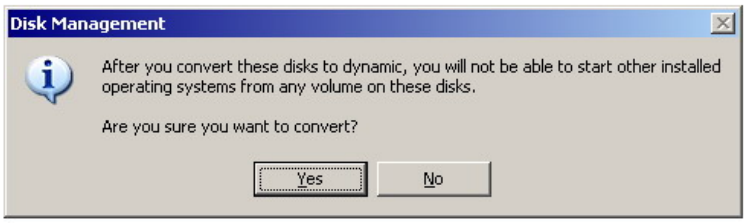
Convert to Dynamic Disk Window Screen

3. In the **Disks to Convert** window, you see an overview of what has been selected. Click **Convert** to confirm.

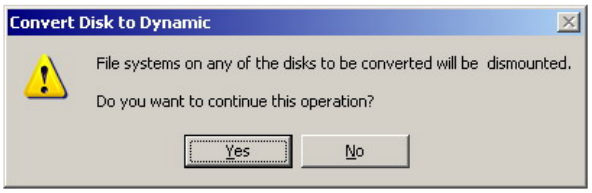


Choosing Disk to Convert Window Screen

4. In the **Disk Management** window, click **Yes** to confirm again.

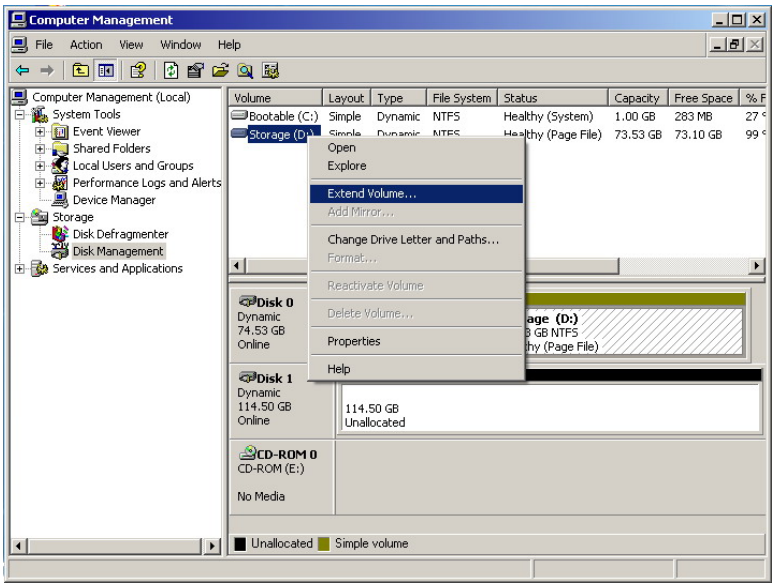

Disk Management
After you convert these disks to dynamic, you will not be able to start other installed operating systems from any volume on these disks.
Are you sure you want to convert?
Yes
No

5. In the **Convert Disk to Dynamic** window, click **Yes** to confirm again.


Convert Disk to Dynamic
File systems on any of the disks to be converted will be dismounted.
Do you want to continue this operation?
Yes
No

6. After the conversion, the system requires a restart.

7. After the WebCCTV has restarted, logon again as **Administrator** and open the **Computer Management** application again. Select **Disk Management** from the left pane. In the right pane, right click **Storage (D:)** and select **'Extended Volume…'** on the popup menu.

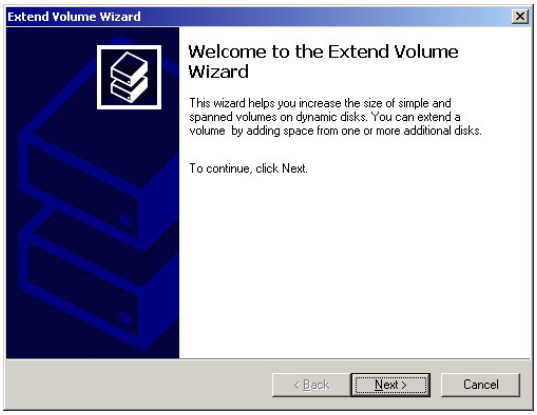


Extending Hard Disk Volume Screen

During this step, it is possible that instead of the graphic shown above, that you may get a graphic that displays: Bootable (C); Bootable (F); Bootable (D); Bootable (G).

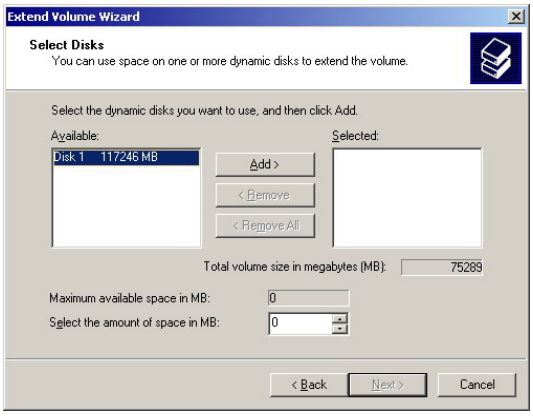
You will need to remove everything from Drive 2 before you start the expansion. To do this, click on the bottom pane of the Disk Manager on each of the F and G partitions and select Delete Partition. When you have no partitions on Disk 2 you may proceed to Step 12.

8. The **Extended Volume Wizard** opens. Click **Next >.**


Extend Volume Wizard
Welcome to the Extend Volume Wizard
This wizard helps you increase the size of simple and spanned volumes on dynamic disks. You can extend a volume by adding space from one or more additional disks.
To continue, click Next.
< Back
Next >
Cancel

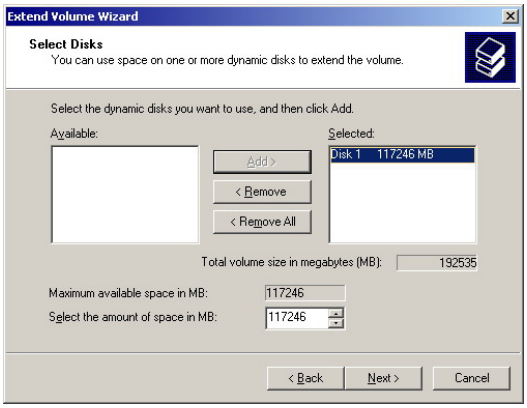
Extend Volume Wizard Screen

9. In the **Extended Volume Wizard**, select **Disk 1** in the **Available** listbox. Click **Add >.**



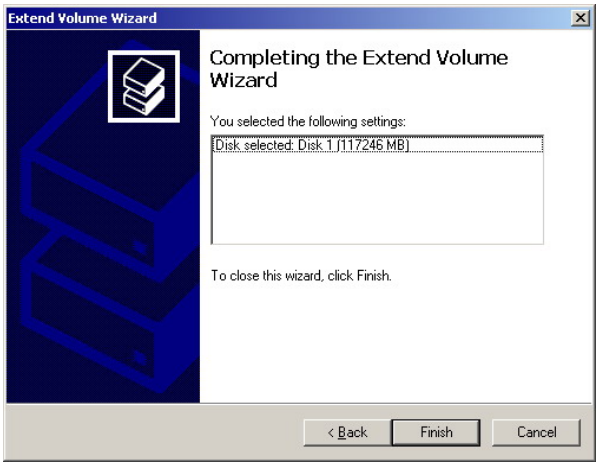
Extend Volume Wizard Screen

10. In the **Extended Volume Wizard**, **Disk 1** has moved to the **Selected** list box. Click **Next >** to continue.



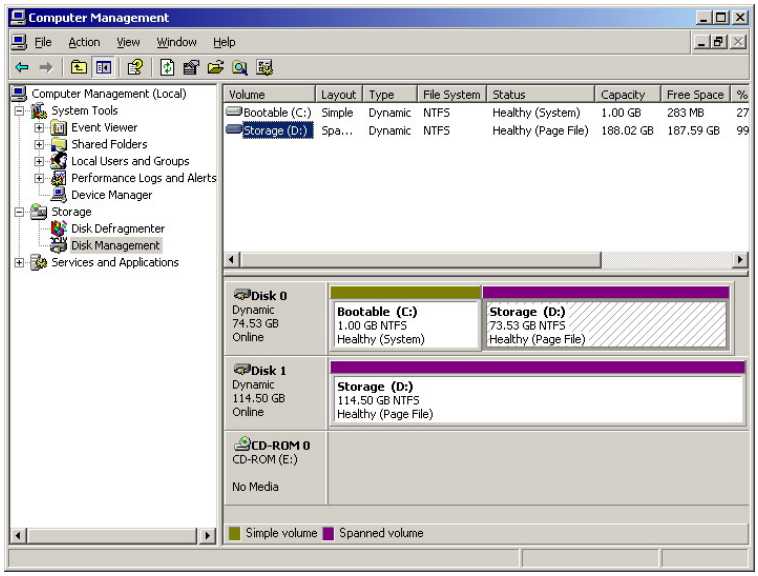
Extend Volume Wizard Screen

11. In the **Extended Volume Wizard**, click **Finish** to confirm



Extend Volume Wizard Screen

12. Eventually the **Computer Management** windows should look like this picture. Note that the capacity of **Storage (D:)** is now the sum of a part of physical **Disk 0** and the whole physical **Disk 1**.



Computer Management Screen

4.2 Video Client Component (ActiveX)

Having a correct installation of the Video Client component is an essential part of a successful GuardNVR installation. Problems like black images appearing, no images appearing at all and errors in Internet Explorer can be the result of an incorrect Video Client Component installation.

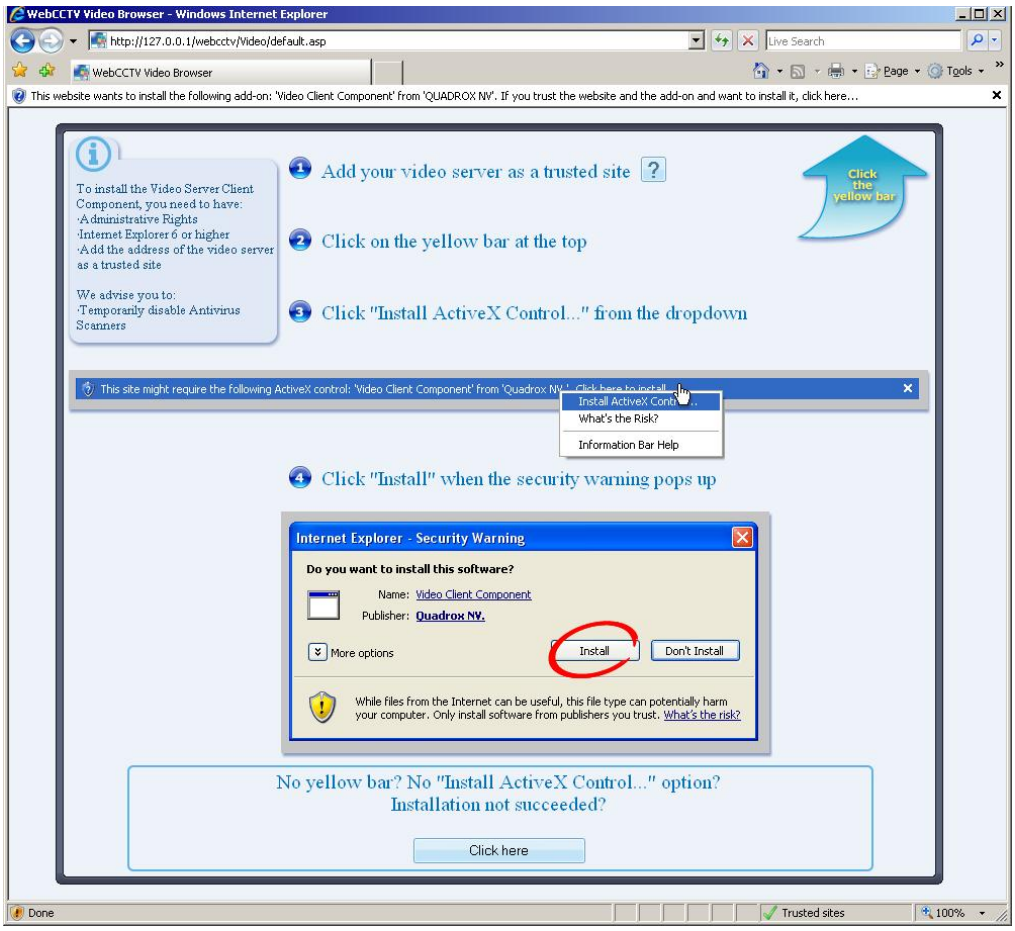
This Video Client Component is based on ActiveX technology. ActiveX is an architecture that lets a program (the ActiveX control) interact with other programs over a network (such as the Internet). In our case the Video Client Component communicates with the GuardNVR and shows video images.

An ActiveX control can be integrated into various environments like a web page. When an ActiveX is integrated into a web page as in the GuardNVR web application, the first time a client machine accesses this web page with Internet Explorer the ActiveX needs to be downloaded and installed on the client machine. At this stage there are several potential problems for the installer to be aware of:

- The Windows user account under which this web page is accessed doesn't have enough rights to install the ActiveX component on the client system. This results in not seeing images at all.
- The security settings of Internet Explorer prohibit the installation of the ActiveX. Add the site to the **Trusted sites** before installing the ActiveX.
- Spyware blockers or anti-virus programs don't allow the installation of an ActiveX on the client machine.
- The Video Viewer ActiveX utilizes various other Windows System components. If any of these system components are incorrectly installed or not present, at all the ActiveX will fail to install or work incorrectly.

It is important that the ActiveX installation is monitored carefully. This has to be performed only once during the first time that the GuardNVR web application is accessed. If something goes wrong during this installation, a user can end up with an incomplete installation of ActiveX.

The installation of the Video Client Component is (semi) automated. When connecting the first time to GuardNVR, a special screen will be shown. Please follow the instructions:


WebCCTV Video Browser - Windows Internet Explorer
http://127.0.0.1/webcctv/Video/default.asp
This website wants to install the following add-on: 'Video Client Component' from 'QUADROX NV'. If you trust the website and the add-on and want to install it, click here...
To install the Video Server Client Component, you need to have:
·Administrative Rights
·Internet Explorer 6 or higher
·Add the address of the video server as a trusted site
We advise you to:
·Temporarily disable Antivirus Scanners
1 Add your video server as a trusted site
Click the yellow bar
2 Click on the yellow bar at the top
3 Click "Install ActiveX Control..." from the dropdown
This site might require the following ActiveX control: 'Video Client Component' from 'Quadrox NV'. Click here to install...
Install ActiveX Control...
What's the Risk?
Information Bar Help
4 Click "Install" when the security warning pops up
Internet Explorer - Security Warning
Do you want to install this software?
Name: Video Client Component
Publisher: Quadrox NV.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?
No yellow bar? No "Install ActiveX Control..." option?
Installation not succeeded?
Click here
Done
Trusted sites
100%

ActiveX Installation Screen

If necessary, the installation manual and setup of the component can be found in the support section of **www.webcctv.com**.

4.3 Changing network ports

This chapter explains how to change different network ports, which are used by a GuardNVR system.

4.3.1 Changing GuardNVR video ports

GuardNVR ships with the default UDP port range set to 4096 – 4223, which are used for video streaming. You may either decrease or increase this range, for that purpose you should change the amount of opened UDP port on your router, firewall and on GuardNVR itself. To change GuardNVR UDP ports go to **Settings->Network Settings**.

The amount of UDP opened ports have to correspond to number of camera streams you want to have simultaneously. For instance, you have GuardNVR with 4 connected cameras, if you launch two GuardNVR clients of GuardNVR simultaneously 16 camera streams will be created (i.e. 4 camera streams for each client) and this doubled because of RTP streaming method. So you have to open 16 UDP ports. **You have to use even numbers for the start and end port of the UDP port range.**

4.3.2 Changing TCP port

GuardNVR ships with the default TCP port set to 80. By maintaining the default setting GuardNVR may be accessed remotely by simply entering either the local LAN address (if accessed from within the network) or the static IP address if accessed from outside the network. If this port needs to be changed, follow the steps below.

1. Logon as **Administrator**.
2. Double Click the **Support** folder from the Windows desktop and select **Internet Information Services** by double clicking.
3. Proceed through the following path **<Computer Name> (local computer)->Websites** and right click **Default Web Site**. Select **Properties**.
4. Under the **Web Site** tab you will find a section **Web Site Identification**. Change the **TCP** port to the desired value and click **OK** to confirm.

When you make a change to a TCP port other than port 80, there are some implications that must be taken into account.

- When you access GuardNVR locally by selecting Video Browser from the desktop, the link http://localhost/guardnvr/browser is launched. This link with have to be renamed as follows if a value other than port 80 is used: http://localhost:xx/guardnvr/browser where xx is the value that you selected.
- When you access GuardNVR from Internet Explorer remotely you would do so by selecting http://xx.xx.xx.xx which is your static IP or internal IP address assuming you

are using port 80 as the default. When you change to a new value, you must now enter http://xx.xx.xx.xx:yy where yy is the new TCP port setting.

4.3.3 Changing remote desktop port

GuardNVR ships with the default remote port set to 3389 that should be forwarded in your router in order to be able to access the unit via remote desktop. If this port needs to be changed, follow the steps below.

1. Logon as **Administrator**.
2. Double Click the **Support** folder from the Windows desktop and select **RegEdit** by double clicking.
3. Proceed through the following path **HKey_Local_Machine->System->Current Control Set->Control->Terminal Server->Winstations->RDP-TCP** Select **RDP-TCP**.
4. After selecting **RDP-TCP**, scroll down the list in the right pane until you come to **Port Number**. Double click **Port Number** to Edit.
5. On the pop up screen select **Decimal** under **Base** and then enter the desired value in the **Value** box.
6. Click **OK** to confirm.
7. Be sure to enter this value in the port forwarding section of your router.

A system reboot is typically required after making registry changes. Check also your **firewall** settings. The new port must be added to the **exception list**.

4.4 GuardNVR power on after power failure

To adjust the GuardNVR server to power on again automatically after the power failure, you must configure the BIOS to go to previous state after power loss. This can be done by entering the BIOS during the initial stage of the machine booting.

4.5 Configuring audio over the Internet

GuardNVR supports specific audio functions for the following brands:

- **Axis** – Listen in and speak:
  - **M1031-W**
  - **P1311, P3301(-V), P3343(-V/VE), P3344(-V/VE)**
  - **Q1755, Q7401**
  - **242S / 243SA / 247S**
- **Panasonic** – Listen in:
  - **BB-HCM311(A), BB-HCM331(A), BB-HCM371(A), BB-HCM381(A), BB--HCM403(A), BB-HCM511(A), BB-HCM515(A), BB-HCM527(A), BB-HCM531(A), BB-HCM547(A), BB-HCM581(A), BB-HCM581A-W, BB-HCM701(A), BB-HCM705(A), BB-HCM715(A), BB-HCM735(A)**

- **KX-HCM110(A)**
- **BB-HCE481(A)**
- **BL-C101(A), BL-C111(A), BL-C131(A), BL-C210(A), BL-C230(A).**
- **BB-HCE481(A)**
- **BL-C101(A), BL-C111(A), BL-C131(A).**

If the installation has a LAN connection, GuardNVR connects to a camera for audio grabbing via the internal address you specified in a camera wizard. If you want to have audio from the camera over the Internet you need to make additional router configuration.

Audio is disabled by default if you add a camera. To enable audio, read the **User manual**.

The following ports should be opened on the router, if not already opened:

- **TCP** Port 80: http
- **TCP** Port 1518: GuardNVR control connection
- **UDP** Ports 4096 till 4223: GuardNVR video streaming

The ports mentioned above are used by GuardNVR ActiveX controls. Since the audio feature operates through the camera's native ActiveX controls (which are installed during the first switching to the camera in Live view) and not the GuardNVR ActiveX and is grabbed from the camera directly a new port for the camera ActiveX controls should be configured as follows:

- Assume that 192.168.1.1 is the camera internal ip-address;
- Assume that 64.160.1.1 is the router external/public ip-address;
- Assume that 6000 port is any free port on your router;
- Assume that 80 port is opened on the camera;

Based on the assumptions above the addressing should be as follows:

64.160.1.1:6000 should be addressed to 192.168.1.1:80

When the router configuration is complete go to the Camera Wizard to add/edit the camera(s) with audio feature, add external IP-address and port you configured as shown on the picture:

Camera Wizard Connection Screen

5 Storage / Bandwidth considerations

Digital video that captures several days or weeks comprises a massive amount of data. If you want to store this data or stream the video over a network, there is a need to reduce the size, because storage devices (hard disks) and networks are limited in capacity.

The size reduction of digital video data is called **compression**: it is a mathematical algorithm (called a **codec**) that is applied to the data. The algorithm carefully removes information that is less important for a human viewer. Because information is lost, inevitably the quality of the videosdf is affected.

There is a trade off between the quality of the video and performance of the system on the one hand, and data size, the compression technique and its parameter on the other hand. The explanation below will help you to make the best choices depending on your specific needs and situation.

For the calculation of an estimate of how long you can record in your situation, refer to the **online storage calculator** on our website:

http://www.webcctv.com/start.asp?main=perf_wizard

5.1 Terminology and basic video technology

This section provides an overview of the terms used in the following sections and the basic underlying technology. It is important that you understand these concepts in order to understand the influence of different factors on quality and size.

A digital image consists of an array of image points, called **pixels**. The amount of points in horizontal and vertical directions is the image **resolution**. Each image point has a certain colour and brightness attached to it, and is represented inside the computer as a number.

If there are more points in an image (higher resolution), more detail will be preserved in the image, but also the necessary space or bandwidth increases.

Digital video consists of series of digital images displayed one after the other. Each image is called a frame, and the speed at which images are displayed is called the **frame rate**. This number is indicated in frames per second (fps).
If more frames are displayed (higher frame rate), objects in the video will move smoother, but also the necessary space or bandwidth increases.

Each number in a computer is represented by a number of 1's or 0's, called bits. The amount of data that a digital video contains per second is called the **bit rate**. This is usually expressed in kilobits (1024 bits) per second (kbps).
For uncompressed video, the bit rate is calculated as:

Resolution x frame rate x colour depth (amount of bits per pixel)

Example: 5 fps of full D1 PAL video:

Bit rate = 768 x 576 pixels/frame x 5 frames/second x 24 bits/pixel
= 53084160 bits/second
= 50,6 Mbps

To illustrate the amount of data that this figure represents, let's see how much uncompressed video we can record on a standard machine with a 250 GB hard disk.

Recording time = 250 Gigabyte x 8 bits/byte x 1024 Megabit/Gigabit / 50,6 Mbps
= 40474 seconds
= 11,2 hours

This number needs to be divided by the number of sources (cameras) that we want to record on 1 system. This is of course unacceptable for a modern video surveillance recorder, which is why we need video compression.

When we stream live video, the video data has to be transported over the network. The capacity of the network to transport data is called **bandwidth**. It is also expressed in kilobit per second (kbps). For network streaming, the rate at which video is transported is more important than the total amount.

When storing video on a hard disk or other storage device, the total storage time is limited by the capacity of the disk. This capacity is determined by the total amount of data that a disk can contain. This is expressed in megabyte or gigabyte.

Please note that for streaming we use **kilobit** while for storage we use **megabyte**.

5.2 Factors that influence bit rate and video quality

There are several factors that have an influence on the amount of data (bit rate), the quality of the video and the performance of the video recorder. The most important factors are explained in this section.

5.2.1 Compression technique (codec)

The biggest influence on quality and data reduction comes from the algorithm that is used to compress the video. Over the years, many algorithms have been conceived, but they can be roughly categorized into two groups:

1. **Intra-fame coding**: each frame is compressed independently of the other frames (e.g. MJPEG).
2. **Inter-frame coding**: since frames are usually very similar, this information is used to further reduce the video size (e.g. WMV, MPEG, H.264)

Inter-frame MPEG-like coding can lead to a bigger compression (typically up to 10 times more video for the same size), resulting in more storage or less bandwidth requirements for the same quality. However, the calculations are more complex, so the performance of the encoding machine will be lower (less streams, more CPU usage).

In general, there is a big difference in performance between doing the compression on the recording device and doing it on the camera or any other specific compression hardware (e.g. a network video server). The latter is highly recommended.

When choosing a particular compression technique, there may be other considerations. For instance, WMV video can be played on any PC running the Windows operating system and on most other devices with video capabilities (e.g. PDA, phone, etc).

Quadrox recommends:

1. For analogue cameras connected to an internal capture board: use WMV7.
2. For network cameras and network video servers: use the native format in which the device streams (no recompression on the recorder).

The chosen compression technique also has an influence on the following discussion.

1. For intra-frame codecs (MJPEG), the quality is usually set by a parameter. As a consequence, frame rate and resolution have a direct influence on the resulting bit rate.
2. For inter-frame codecs, the bit rate is usually a parameter. As a consequence, frame rate and resolution don't have a direct influence on storage and bandwidth requirements, although they might have an influence on the quality of the resulting video.

This means that when the bit rate increases, the resolution will decrease as well as the frame rate. All these parameters together produce a better image quality.

5.2.2 Resolution

When the compression technique is based on JPEG images, a second big factor in data size reduction is the resolution. As mentioned before, compression works by selectively reducing the amount of information in the image. One way to do that is to reduce the size of the image.

Example:
A VHS quality image (PAL) of 384x288 pixels can be considered as a SVHS+ image of 768x576 pixels where you throw away every other pixel in either direction. This reduces the data size by a factor of 4.

Of course, this influences the quality of the image. Especially fine details are more likely to get lost, like face characteristics or details of clothing.

The resolutions that are mentioned, except for the mega-pixel, are for the PAL standard. NTSC images and pure digital images might have a slightly different resolution, but in general the same steps/magnitude apply.

Postage stamp format (192x122). This resolution is offered by some of Quadrox competitors. At this image size however, most of the information in the image is lost. At best, one would be able to count the number of people in the image, but there is no hope for e.g. identifying faces.

VHS quality (384x288). Small and thus favourable for storage and transmission, this resolution gives a good quality in most cases.

SVHS quality (768x288). In this image format, only half of the image is lost. The image is only decimated in the vertical direction. For analogue based cameras, this is the maximum resolution possible without motion artefacts (see below). Best choice for an analogue camera.
Notice that this resolution doesn't have the classical 4:3 proportions. This can be compensated for, but some media players might display a "squished" image.

SVHS+ quality (768x576): This is the maximum resolution for all analogue and most network cameras currently in the market. Most detail is preserved.
This resolution has a big disadvantage though. Because of the video sensor technology inside the camera (interlacing), the image shows horizontal lines at the edges of moving objects. This makes the object (e.g. a face) unrecognizable in most cases and as such seriously diminishes the usability of the camera.

For more detailed technical explanation about interlacing and its consequences, please contact Quadrox support.

Megapixel quality (1280x960 and higher): Network cameras with more than a million pixels are becoming the new type of camera's in today's marketplace. Because of their high pixel count, they can preserve much more detail than a regular camera, making them useful in many circumstances. This comes at a very considerable storage and network bandwidth cost!

As a final remark on resolution, we should reiterate that resolution has quite a different effect when using inter-frame codecs for compression (MPEG, WMV). In these cases, choosing a smaller resolution means less quality (as above), but not less data, since the bit rate is fixed.

For a fixed bit rate, a higher resolution means that information has to be removed in other ways, reducing the image quality.

Keep in mind that choosing a higher resolution also means putting a higher load on your GuardNVR and may reduce its performance. Bigger images need more internal resources like memory and processing time.

5.2.3 Frame rate

When choosing a resolution, we reduce the amount of data by reducing the size of an image. Similarly, we reduce the amount of data by simply storing or streaming fewer images. Frame rate is a third big factor in compression. This factor is potentially big, since the difference in frame rates can range from 30 fps to one image every 3 seconds, a factor of 100!

When reducing the frame rate, the loss of quality creates video that is not “smooth”. The human eye needs a certain frame rate to perceive a sequence of images as smooth motion. When reducing the frame rate to a number below this amount, the image “shocks”. However, while being less pleasant to look at, the quality of the individual images is not affected, so all detail is preserved.

The threshold of the human eye for perceiving a sequence of images as smooth motion lies at about 15 images per second, depending on the person. Although the broadcast industry (television, DVDs, film, etc) take a substantial margin on this with streams at about 25 fps, this is not absolutely necessary for smooth motion.

Because of this, streaming at more than 15 fps is almost never useful and mostly serves to increase your bandwidth requirements. In most cases, even 10 or 12 fps suffice for a satisfactory viewing experience.
For recording, frame rate is usually reduced further, since nothing much occurs in the time period of $1/15^{th}$ of a second. A storage frame rate of 3 to 6 fps is enough for most practical applications.

Similar remarks about the relation between compression technology and frame rate hold as they did for resolution. When using (M)JPEG, frame rate has a direct influence on bit rate since each image is compressed separately. When using MPEG, H.264 or WMV, the bit rate is set, so frame rate potentially has an influence on quality rather then on data size.

5.2.4 "Differential" live streaming

In order to further reduce the bandwidth requirements for live streaming, Quadrox engineers have devised an extra algorithm that can improve the JPEG streaming for analogue cameras. When using differential live streaming, only the parts of the image that actually change visually are transmitted to the viewing component. At the receiver side, the parts of the image are recombined into a full image. In terms of quality, this form of data size reduction can hardly be noticed, but the bandwidth is reduced drastically. This allows us to stream high quality video over a lower quality bandwidth.

If you want to remotely access the GuardNVR video server over the Internet, it is highly recommended to use differential streaming. Another possibility is using Low Bandwidth streaming. More info can be found in the User Manual.

This feature is not available for network cameras. Low Bandwidth streaming is available for both analogue and network camera's.

5.2.5 Activity detection for storage

For storage, we can apply a similar principle. Only the images that have meaningful activity in them need to be stored. When nothing is happening, recording can be suspended. To better distinguish meaningful activity from "background movement" (e.g. a street nearby, a moving tree), masking can be applied to take only certain parts of the image into account.

This technique not only reduces the storage requirement, but also makes it much easier to trace important events in the recordings afterwards, saving you both money (hardware) and time.
Using activity detection is highly recommended in almost all cases. Typically, it allows you to increase storage time up to 400%. For cameras with little motion, e.g. in an empty hallway in an industrial facility, it can even reduce the storage space to about 1% of the original volume!

6 Security Policy

This chapter describes guidelines for proper use and a security policy, which are designed to ensure the proper functioning of a GuardNVR video recorder and to provide a guideline for protection against hackers, viruses, malware and other forms of electronic attacks.

Quadrox will not support any problems that arise from not complying with the guidelines and policies in this chapter.

This chapter is structured in three major parts.

First, the guidelines for proper use of GuardNVR are explained. GuardNVR is a dedicated system that should be used solely for the purpose of video recording and surveillance.

Secondly, the details of the security policy are outlined. To sum it up in a single sentence, the policy amounts to this: We will lock down GuardNVR as much as possible, leaving as few places as possible where an attack could occur, and securing the remaining places as much as possible. We will provide you with information about how we lock the machine and how you can open it if necessary. As mentioned above, Quadrox will not support this any further.

Thirdly, some additional ways to recover from errors are explained for your convenience.

6.1 Proper use of GuardNVR

GuardNVR is a dedicated system that should be used solely for the purpose of video recording and surveillance. Since the GuardNVR server has Windows XP/Vista as its operating system, it can be accessed locally and used as a normal PC. There are several precautions, which prevent improper working of the system.

GuardNVR software should be used in conjunction with dedicated software (i.e. such usage should be agreed to with Quadrox) or with software that doesn't cause:

- A high CPU and memory load on the GuardNVR server (i.e. CPU consumption, memory of all types consumption, etc.), which could hinder the proper working (including video quality) and could shorten the uptime of GuardNVR server software.
- The installation of viruses, spyware, adware, malware and other forms of software that form a threat against the health of GuardNVR server software.
- GuardNVR server software malfunction (if such consequence is known beforehand).

The precautions put above will help to increase the security and ensure proper functioning of GuardNVR throughout its lifetime.

6.2 Security policy

At the start of this section, let's repeat the basic premise of the GuardNVR security policy:

Lock down GuardNVR as much as possible, leaving as few places as possible where an attack could occur, and secure the remaining places as much as possible.

"Locking down" the GuardNVR means that you should try to prevent malicious attacks on GuardNVR by not giving attackers (hackers, viruses, etc) the possibility to exploit weaknesses in the system.

GuardNVR uses the Microsoft Windows XP/Vista operating system. Like any other operating system including Linux and other Unix variants – or any software for that matter – this operating system is not perfect. It contains certain weaknesses that could be used to get unauthorised access to the machine.

Generally speaking, Windows XP/Vista is a very safe operating system when administered correctly. There are several ways outlined in this section to increase security.

- Have secure passwords.
- Don't leave GuardNVR under the administrator account logged on.
- Keep the system up to date.
- Secure the network access.
- Make sure that any other access doesn't cause problems.

Contrary to popular believe, most attacks on computer systems are not brute-force attacks by extremely skilled people on a weak operating system. Instead, most attacks exploit vulnerabilities that were created "from the inside". This implies that you have control over the situation and can prevent attacks by rigorously securing the machine and being careful when handling it. In the next paragraphs, you can find out how to do this.

6.2.1 Password policy

The very first thing that you should do after installing GuardNVR, is to change the Administrator password!

To avoid passwords leaking out of the organization or being retrieved otherwise, follow these guidelines:

- Publish passwords to as few people as possible. The fewer people knowing the password, the less chance of it ending up with the wrong person.
- Don't keep passwords in written form in places that might be accessible by malicious people. This includes paper documents that might get lost, websites, mail and IM messages.

- Restrict the number of Administrators to a minimum. Since users have fewer rights, a user password leaking has fewer severe consequences. It is even advisable to have an extra user account for each administrator, which should be used for regular viewing.
- Choose strong passwords. A strong password is a password that is hard to guess by attackers (people and software). This helps to secure the product against brute force attacks (trying all passwords). Use the following guidelines:
    - The password should be at least 8 characters long. Longer is better.
    - Use both CAPTIAL and small letters (at least one of each).
    - Use both letters and figures or other characters (at least one of each).
    - There should be no connection whatsoever between the username and the password. This includes copying parts of the username or having a semantically relevant meaning (e.g. the password is the name of the user's wife). Preferably, the password should have no "human" meaning at all.

One of the prime ways for hackers to retrieve passwords is simply asking for it. A hacker would pretend to be e.g. a support technician and ask you for the password. In order to prevent this kind of attack, we outline here the procedure for Quadrox support people regarding passwords of customers.

First of all, by default Quadrox does not know any passwords of machines in the field. Since we use the operating system for authentication, there is no way in which we can retrieve a password, for any reason. The only way for us to know a password is if the customer voluntarily tells us.

If it is necessary for Quadrox support to have the password in order to give assistance, the support technician will ask the customer to call the general Quadrox support number or use the official support@quadrox.com (.be) address. This way, the customer is sure that he tells the password to the correct person.

When you have the slightest doubt about the authenticity of the support person, the requested way of communicating the password or the telephone number given to call, please don't hesitate to call Quadrox support on the following number: +32 (0)16 58 25 85. For USA customers, please call 1-888-QUADROX.

The Quadrox support personnel will not save or keep passwords in any way. For optimal security you should change the password after a support call, or in general after revealing the password to anyone who normally doesn't have access.

Default passwords should be changed as soon as possible, preferably even before GuardNVR is put on the network. Otherwise attackers can gain access to the system using easily retrievable passwords. It's like locking the door, but leaving the key in the lock.

6.2.2 Windows security updates

To keep your system secure, it is important that you keep it up to date. This will prevent an attacker from using vulnerabilities that have already been removed by Microsoft.

Quadrox is not responsible for keeping the installed GuardNVR software and Windows OS up to date. This is the responsibility of the installer. Quadrox is not responsible for problems that originate from not keeping the machine up to date (patches until the last release applied). If such a problem occurs (e.g. a virus), Quadrox will recommend a full re-installation.

6.2.3 Network security

The network is the main interface of GuardNVR, through which an attack can occur. That's why it is important to pay special attention to its security.

In accordance with our general security policy, we will try as much as possible to limit the way in which the network can be used, while not interfering with GuardNVR functionality. There are several ways to limit the network:

- Physical limitation (dedicated network)
- Limiting the number of connections (LAN versus Internet)
- Using only one network protocol (TCP/IP)
- Allowing only traffic on the necessary network ports (Firewall)
- Allowing only known clients
- Limiting the functionality of the web server (securing IIS)

6.2.3.1 Dedicated network versus integration with the corporate network

Having a dedicated network for video surveillance, adds an intrinsic level of security by physically eliminating access points for attacks. This way, you can easily have a safe and robust system. The network becomes a safe entity in itself, while if GuardNVR is incorporated in a more general network, security should be built around the GuardNVR server.

A dedicated network also ensures that the video traffic doesn't interfere with other general data. This potentially increases the performance of both GuardNVR and other applications on the network.

On the other side, integrating the video network with the corporate network can potentially reduce the costs of installation and administration. Both solutions are possible and endorsed by Quadrox. The choice depends on your performance, cost and security needs.

6.2.3.2 Connecting GuardNVR to the Internet

When GuardNVR is in a LAN, the number of network nodes from which an attack can originate is at most a couple of hundred. When GuardNVR server is connected to the Internet, this number rises to millions instead. Connecting GuardNVR to the Internet dramatically increases the chance on an attack.

The choice of putting a unit on the Internet depends on the needs of the end user, but if you do so, please pay extra attention to the security issues mentioned in this document.

6.2.3.3 Limiting the number of protocols

By default, the Windows operating system supports multiple network protocols. An example is NetBios which is, among other things, the protocol used to share folders across the network.

To increase security Quadrox recommends disabling these protocols on a GuardNVR server. Only one protocol is recommended to be enabled: TCP/IP. This is the main protocol used on most of the current networks, including the Internet, and the only one needed for GuardNVR functionality.

Disabling other protocols prevents attacks that use them and it is in that sense a good measure to increase security. Furthermore it prevents the unit from broadcasting, or in other words constantly yelling its position to the rest of the network. This makes it more difficult for an attacker to find the unit on the network, which again increases security.

In some exceptional cases it might be necessary to enable these protocols again, e.g. to backup video through shares. This is technically possible: the protocols are disabled, not removed. However, Quadrox strongly advises against this practice and will not give support on this functionality or any problems that originate from it.

6.2.3.4 Firewall

A critical element in GuardNVR security is the firewall. A firewall is a piece of software that basically allows only a limited number of applications to use the network.

GuardNVR may use Microsoft firewall, which is enabled by default in the Microsoft XP SP2 and Vista operating system. It is a basic firewall with limited functionality, but none the less effective for our goals.

Only the following applications are recommended to be allowed:

- Web server needed for the web application (IIS, TCP port 80)
- GuardNVR video server software (OPServer and OPVWSYS, TCP port 1518 and UDP ports 4096-4223)
- Remote desktop needed for remote administration and support

This is only valid for connections that are made to GuardNVR. For outgoing connections (connections made from GuardNVR server to another machine) there is no restriction. However, please follow the guidelines for proper use to prevent problems.

In some exceptional cases it might be necessary to allow more applications (open more ports). This is technically possible; however, Quadrox strongly advises against this practice and will not give support on this functionality or any problems that originate from it.

6.2.3.5 Allowing only known clients

If you have a set-up with a fixed number of known clients, there is a possibility to only allow these clients, based on their IP address. No other clients will be allowed to access GuardNVR. This would further limit the number of possible connection points and thus increase security.

This is only usable in a limited number of scenarios and can give rise to a number of logical problems. Please contact Quadrox support for more information.

6.2.3.6 Securing the applications

When applying the restriction on applications with the firewall such as explained above, the attackable points are effectively limited to those applications. In the next step we should make sure that those applications themselves are secure.

Remote desktop doesn't have ways of automation. This implies that only a human operator can use it, not a piece of software like a virus. The risk of a human operator performing malicious actions is limited to the access he has. The security of this falls back to the security of the passwords, for which a policy is outlined above.

The GuardNVR server is an unlikely point of attack, since it is not a wide spread application like a web server. This means that very few people would be interested in designing an attack on this software. Those people would have to know a lot about the internal workings of the server, which is difficult. This being said, Quadrox engineers are working hard to keep the number of possible security risks to an absolute minimum.

Only one application remains, namely the web server (IIS). Quadrox uses tools issued by Microsoft like urlscan and lock-down to block any action that is not related to GuardNVR functionality. To ensure security of IIS, please make sure that all necessary security updates are applied (see above).

6.2.3.7 VPN

Setting up a virtual private network (VPN) can potentially increase security, similar to having a dedicated network or limiting the clients on IP address. It uses encryption of data that goes over the network to achieve this goal.

Setting up a VPN for your video surveillance equipment is outside the scope of Quadrox support. Be aware that the encryption process can cause delays that might affect the performance of the video system.

6.2.4 Other types of access

Apart from the network, there are several other ways in which a malicious piece of software can end up on GuardNVR. These ways include all information carriers that can be connected to GuardNVR servers, like CDs, floppies and USB memory drives.

When connecting these information carriers to GuardNVR server, pay special attention to security. Make sure that they are scanned for viruses and malware before connecting them.

Along the same line of reasoning you should pay extra attention when you introduce foreign objects in a shielded environment, e.g. a laptop of a technician in a dedicated video network.

6.2.5 3rd party security tools

When the machine is locked down like described above, it should be resistant against the majority of threats. The limited increase in security that would be achieved by pre-emptively introducing additional security tools probably does not justify the additional cost of licenses and efforts for installation and maintenance. Furthermore, this software might interfere with the functionality of GuardNVR.

Such tools include virus scanners, malware/spyware/adware removal tools, additional pop-up blockers, firewalls with extended functionalities, script blockers, etc.

As a general guideline, script blocking should be disabled at all times, since GuardNVR uses scripts to implement its functionality. The 3rd party tools also need to allow the proper installation and execution of signed ActiveX components.

6.3 Error recovery mechanisms

GuardNVR has the ability to automatically recover from common problems like crashes, overheating, etc. This is achieved through: System Health Service (SHS).

System Health Service is software running on GuardNVR as a service. It monitors the hardware and some vital processes on the machine, like the GuardNVR server and IIS. If something happens (e.g. a crash) to any of these processes, the SHS will try to recover by – depending on the seriousness of the situation – restarting the process or rebooting the PC.

7 Troubleshooting

GuardNVR is a reliable system and is designed and tested for durability. However, problems may occur, following procedures in this chapter can help to determine the cause.
You should become familiar with this chapter. Knowing what might go wrong can help prevent problems from occurring.

7.1 Problem solving process

Resolving problems will be much easier if you observe the following guidelines:

- Stop immediately when you recognize a problem exists. Further action may result in data loss or damage. You may destroy valuable problem-related information that can help solve the problem.
- Observe what is happening. Write down what the system is doing and what actions you performed immediately before the problem occurred.

The questions and procedures offered in this chapter are meant as a guide, they are not definitive problem solving techniques. Many problems can be solved simply, but a few may require help from your installer. If you find you need to consult your dealer or other consulting person, be prepared to describe the problem in as much detail as possible.

7.1.1 Preliminary checklist

Consider the simplest solution first. The items in this section are easy to fix and yet can cause what appears to be a serious problem.

- Make sure you turn on all peripheral devices. This includes your printer and any other external device you are using.
- Before you attach an external (none USB) device shut down the GuardNVR. When you turn the GuardNVR back on it recognizes the new device.
- Make sure all options are set properly in the corresponding setup program.
- Check all cables. Are they correctly and firmly attached? Loose cables can cause signal errors.
- Inspect all connecting cables for loose wires and all connectors for loose pins.
- Check that your CD/DVD-ROM is correctly inserted.

7.1.2 Analyzing the problem

Sometimes the system gives clues that can help you to identify why it is malfunctioning. Keep the following questions in mind:

- Which part of the system is not operating properly: keyboard, hard disk drive, optical media drive, or display? Each device produces different symptoms.
- Is the system configuration set properly? Check configuration options.
- Do any indicators light? Which ones? What colour are they? Do they stay on or blink? Write down what you see.
- Do you hear any beeps? How many? Are they long or short? Are they high pitched or low? Is the GuardNVR making any unusual noises? Write down what you hear.

Record your observations so you can describe them to your dealer.

7.2 Solutions for common problems

7.2.1 Start up problems

Problem	Possible causes and resolutions
Nothing shows up on the monitor when you try to start GuardNVR	• Monitor problem o Check the section on monitor problems • Boot problem o Check the rest of this section
GuardNVR doesn't switch on	This is probably caused by a lack of power. • Cable not connected or damaged o Make sure that the power cable is firmly connected to the GuardNVR power supply and to a working power outlet. o If the cable is frayed or damaged, replace it. o If the cable connectors are dirty, wipe them with cotton or a clean cloth. • Power outlet isn't operational o Contact the building manager. • Power outlet doesn't have the correct voltage o Adapt the jumper switch on the power supply to match the power outlet voltage. • Power supply is in safety mode because the GuardNVR overheated o Let the unit cool down and try again. Locate the source of the overheating and eliminate it • Power supply is broken o Contact your hardware distributor
GuardNVR boots from another storage device then the hard disk (e.g. CD-ROM)	• The BIOS settings are not appropriate o Remove the storage device (e.g. take the CD-ROM out of the CD-ROM drive) o Adapt the BIOS settings to boot from the hard disk first
"No system disk" is displayed	The GuardNVR doesn't find a suitable storage device to boot from. • No operating system is installed on the hard disk • The hard disk malfunctions o Check the cables which connect the hard disk to the motherboard o Contact your hardware distributor

GuardNVR doesn't boot and emits beep sounds	A hardware device malfunctioned. • The RAM memory malfunctions o Check if the RAM memory is correctly inserted o Replace damaged RAM memory o Replace any RAM memory that is not compatible with the GuardNVR o Contact your hardware distributor • Another component malfunctions o Contact your hardware distributor
The keyboard or mouse doesn't function	a) The lights (LED) on the input device don't function. • Cables not properly connected o Make sure that the mouse or keyboard cable is firmly connected to the GuardNVR • Input device broken o Check the mouse or keyboard on another PC b) The lights (LED) on the input device function, but there is no reaction on movement. • Input device connected by PS/2 o Reboot the unit • Input device connected by USB o Disconnect the device and connect it again

7.2.2 Monitor problems

Problem	Possible causes and resolutions
The monitor is completely black	• Monitor switched off o Turn on the monitor • Cable not connected or damaged o Make sure that the power cable is firmly connected to the monitor a working power outlet. o If the cable is frayed or damaged, replace it. o If the cable connectors are dirty, wipe them with cotton or a clean cloth. • Monitor set up to complete darkness o Try to adapt the brightness and contrast settings of the monitor • Monitor broken o Try another monitor
The monitor displays an error (e.g. “No signal”)	• Monitor cable not properly connected o Make sure that the monitor cable is firmly connected to the GuardNVR and to the monitor
The monitor doesn’t display correct colours	• Monitor cable not properly connected o Make sure that the monitor cable is firmly connected to the GuardNVR and to the monitor • Monitor set up incorrectly o Try to adapt the brightness and contrast settings of the monitor

For other problems, please check the documentation of the monitor manufacturer.

7.2.3 Windows logon problems

Problem	Possible causes and resolutions
You forgot the password of a User	• Log in as Administrator, reset the Operator’s password through the web application
You forgot the password of the Administrator	• Re-install the GuardNVR Since Quadrox uses the Windows Operating System for authentication, there is no back door to retrieving or resetting the password.

The password is not accepted	• Incorrect spelling o Type the password again o Pay special attention to capital letters, the password is case sensitive! • Incorrect keyboard settings o Type Ctrl-Shift to switch your keyboard settings, if you have set up multiple keyboard configurations o Use an appropriate keyboard

7.2.4 Remote connection problems

Problem	**Possible causes and resolutions**
Internet Explorer shows HTTP error 404 "The page cannot be found"	• IP address or domain name incorrect (spelling mistake) o Correct the spelling and try again • No physical connection to the GuardNVR You can test this by performing a ping test o Check if the network cable of the GuardNVR is properly connected to the NVR and to the switch, hub or router o Make sure the switch, hub or router is turned on and working o Try to connect the GuardNVR to a different port on the switch or hub • A 3rd party application (e.g. a virus scanner) is preventing the page from being displayed o Disable the 3rd party software and try again • IIS (Internet Information Service) is not running properly o Contact Quadrox support
The Welcome screen appears, but the logon screen doesn't	• Scripts are blocked o Disable any script blockers, including script blocking functionalities of anti-virus software o Make sure port 1518 is opened. o Make sure the GuardNVR server is added to the Trusted Sites list of Internet Explorer.
A message pops up: "Your security settings prohibit running ActiveX controls on this page. As a result the page may not display correctly."	• Internet explorer blocks the installation of the ActiveX component o Configure Internet Explorer to allow the installation and execution of signed ActiveX controls o Add your GuardNVR to the trusted sites list.

Browser returns 'connection refused'-like message	• Internet Explorer has a proxy server enabled in the Internet Options, which blocks URLs like 'localhost' o Remove the proxy server from the Internet options: Tools > Internet Options > Connections > LAN Settings.
A message pops up: “The connection was actively refused by the GuardNVR server.”	• Your firewall blocks GuardNVR signals o Check whether all firewalls (server and client side) are correctly configured.

7.2.5 Camera problems

Problem	**Possible causes and resolutions**
No or unstable images	• Camera not properly connected o Check the connections (network, coax cable) o If the cable or connectors are damaged, replace the cable. o In case of analogue cameras, check whether the cable is under voltage • Camera is turned off o Connect the camera to a working power outlet o Turn on the camera
The image is out of focus or trembles	• Lens is not properly adjusted o Try to adjust the camera to show more a focused picture. • Camera not properly connected o See above for resolutions

For other problems, please check the documentation of the camera manufacturer.

7.2.6 GuardNVR software problems

Problem	**Possible causes and resolutions**
The buttons of the web application don’t work	• Internet Explorer hangs up o Close the browser and try again • GuardNVR server malfunctions o Restart the server with the icons on the GuardNVR desktop o If the problem persists, reboot the GuardNVR o If the problem persists, contact Quadrox support

A black image is shown	• DirectX not installed or outdated Check by Start > Run, type “dxdiag”. The DirectX version should be at least 9.0c o Download and install the latest DirectX version from http://microsoft.com/directx • Video drivers of the client computer are outdated o Download the latest video drivers from the website of the client computer manufacturer • Firewall blocks image transfer o Check whether all firewalls (server and client side) are correctly configured.
No grid is displayed in the activity detection screen.	• Video card has less than 16 MB of video memory. Go to the Display settings, go to the Settings tab, click Advanced. A new window appears, click the Adapter tab. Check that Memory Size is at least 16 MB. • DirectX 9.0c or higher is missing o Download and install the latest DirectX version from http://microsoft.com/directx • Not enough hardware acceleration o See the section on client configuration
Very bad image quality (image shows big planes of the same color)	• The color depth in the display settings isn't set to 24 or 32 bits o Change the color depth to 24(32) bits instead of 16 bits in the display properties. Right click on the Desktop, choose Properties. Go to the Settings tab, and set the color depth to 24(32) bits. • Wrong combination of graphics controllers and/or drivers o Contact Quadrox support
PTZ supporting camera doesn't have PTZ	• Problem with camera configuration (source numbering) o Delete all IP devices. Add them again using the Camera Wizard. Make sure to add the cameras per brand and per type, not alternating different brands or types!

7.3 If you need further assistance

If you require any additional help using your GuardNVR or if you are having problems operating the GuardNVR, you may need to contact Quadrox for additional technical assistance.

7.3.1 Before you call

Some problems you experience may be related to software other than GuardNVR or the operating system. It is important to investigate other sources of assistance first. Before contacting Quadrox try following:

- Review troubleshooting sections in the documentation for other software and peripheral devices.
- If a problem occurs when you are running other applications, consult the documentation for that software for troubleshooting suggestions.
- Consult the dealer you purchased software from. This way is the best source for current information and support.

7.3.2 Collecting the necessary information

When you contact Quadrox for technical support, you will be asked to provide the following information. Please have this information ready before you call and include it in every email that you send. This will help the support people to handle your problem in the most efficient way. All information is obligatory.

All this information can be gathered by one simple click in the Video Manager → Info -> **Generate System report**. Save the file and send it to support. Check the **User Manual** for more information about this topic.

- ***What is the type of product?***

Possible types are WebCCTV, Guard, Enterprise… installation. The type matches the name in the Windows Start menu.

- ***How many units are showing the problem?***

- ***How many video sources are connected to each unit?***

Make a distinction between the different types (brands) of network cameras and network video servers. You can find this information in the web application. Log in as Administrator and go to the “System” menu. There you will find a list of the connected sources.

- ***What is the version of the operating system?***

- ***What is the version of your GuardNVR software?***

This information can be found in the web application. Log in as Administrator, go to the “System” menu and select “System info”. The numbers that you need to provide are “XPe build version” and “Setup version”.

- ***What is the problem?***

Please make sure that you have the relevant information concerning your problem. What is going wrong? What were you expecting? A good problem description can help the support person to handle your question more efficiently.

All this information can be gathered by one simple click in the Video Manager → Info -> Generate System report. Save the file and send it to support.

7.3.3 How to contact Quadrox

If you are still unable to solve the problems and suspect that it is related to the GuardNVR products, contact Quadrox as described in the Appendix B Contact Us.

USA:

E-mail:	support@quadrox.be
Telephone:	+1 888 QUADROX

Europe:

E-mail:	support@quadrox.be
Telephone:	+32 (0) 16 58-25-85
Fax:	+32 (0) 16 58-25-86

7.3.4 How to allow remotely access to your GuardNVR by Quadrox support

Sometimes to fix a problem with your GuardNVR unit the easiest way for Quadrox support is to take remote control of your GuardNVR. Quadrox support will only attempt this after having been in contact with you through phone or email. Remote Access to the GuardNVR is established with the help of the Quadrox Remote Assistence Tool, VNC, RDC, Logmein or CoPilot (www.copilot.com).

8 Appendices

Appendix A

GuardNVR installation checklist

Please check that you performed all steps listed below:

① Hardware connections:

1. Connecting the power outlets to the GuardNVR, cameras and the network switches.
2. Establishing a network connection between all of the devices by connecting each of them to a network switch using UTP network cables

② Configuring the GuardNVR's IP-address

③ Configure the cameras by:

1. Giving all cameras a ***static*** **IP address** using the Camera Setup CD-ROM.
2. Giving all cameras a user name and password.
3. Adding all the cameras to the GuardNVR Web Application using the correct static IP address, user name and password assigned in the steps above.
4. Setting all the camera parameters, such as the camera quality (resolution), recorded frames per second and compression type.
5. Setting the activity detection level & masking correctly.

④ Checking for the presence of recordings for all connected cameras storage folder you selected during installation.

⑤ Verifying the combined CPU consumption of the GuardNVR is not higher than 55% when all connected cameras are simultaneously recording.

⑥ Changing the default passwords into strong passwords. The passwords are changed in the User management of the GuardNVR application.

⑦ Checking access to the GuardNVR from a remote unit of the network.

⑧ Saving the GuardNVR settings using the **Save Configuration** feature in the **System info** screen.

⑨ Configuring a router (not needed when the GaurdNVR is not accessed from an external location)

- Opening TCP ports 1518 and 80.
- Opening the UDP port range 4096 ~ 4223
- Opening the TCP port 3389 (and 5500) for outgoing (optional)
- Forwarding all of the above ports to the internal IP address of the GuardNVR
- Above are the default ports. Note that these ports change when the default ports are changed in the GuardNVR settings
- Checking the Internet connection.

Appendix B

Contact Us

Quadrox is a leading provider of Digital Video Internet infrastructure management solutions, enabling companies to leverage the Internet to deliver better physical security and more powerful and cost-effective Digital Video applications and services to their customers, employees and business partners. The Quadrox GuardNVR product family provides an efficient and reliable infrastructure by which enterprises can distribute, update and manage video sources and content over corporate intranets, extranets and the Internet.

Corporate headquarters

Belgium:

Address:	Quadrox tsov., Duigemhofstraat 101, 3020 Herent, Belgium
Telephone:	+32 (0) 16 58-25-85
Fax:	+32 (0) 16 58-25-86
E-mail:	info@quadrox.be

USA:

Address:	Quadrox US 900 Warm Springs Road, Ste. C102 Henderson, Nevada 89011
Telephone:	(+1) 702-564-6340
Toll Free:	(+1) 888-564-6340
Fax:	(+1) 702-564-6341
E-mail:	info@quadrox.com

Technical support

Quadrox is committed to providing you with the best overall product experience. This includes intuitive technical products and flexible options to fit your support needs. Our products are designed with superior quality and ease of use in mind, but we understand that issues do arise from time to time that need the backing of our support resources.

USA:

E-mail:	support@quadrox.be
Telephone:	+1 888 QUADROX

Europe:

E-mail:	support@quadrox.be
Telephone:	+32 (0) 16 58-25-85
Fax:	+32 (0) 16 58-25-86

Appendix C

Camera protocols supported by WebCCTV

Updated on: 19 October, 2009

IP cameras

ACTi

- Acti ACD-2100 PAL
- ACTi ACD-2100 NTSC
- ACTi ACM-1100N
- ACTi ACM-1100P
- ACTi ACM-1101N
- ACTi ACM-1101P
- ACTi ACM-1111N
- ACTi ACM-1111P
- ACTi ACM-1231
- ACTi ACM-1232
- ACTi ACM-1311N
- ACTi ACM-1311P
- ACTi ACM-1431N
- ACTi ACM-1431P
- ACTi ACM-1432N
- ACTi ACM-1432P
- ACTi ACM-1511
- ACTi ACM-3001
- ACTi ACM-3100N
- ACTi ACM-3100P
- ACTi ACM-3101N
- ACTi ACM-3101P
- ACTi ACM-3111N
- ACTi ACM-3111P
- ACTi ACM-3211N
- ACTi ACM-3211P
- ACTi ACM-3311N
- ACTi ACM-3311P
- ACTi ACM-3401
- ACTi ACM-3411
- ACTi ACM-3511
- ACTi ACM-3601
- ACTi ACM-3603
- ACTi ACM-3701
- ACTi ACM-3703
- ACTi ACM-4201
- ACTi ACM-1011
- ACTi ACM-3011
- ACTi ACM-4000
- ACTi ACM-4001
- ACTi ACM-4100 NTSC
- ACTi ACM-4100 PAL
- ACTi ACM-4200
- ACTi ACM-5001
- ACTi ACM-5601
- ACTi ACM-5611
- ACTi ACM-5711N
- ACTi ACM-5711P
- ACTi ACM-7411
- ACTi ACM-8201
- ACTi ACM-8211
- ACTi ACM-8511 NTSC
- ACTi ACM-8511 PAL
- ACTi CAM-5200HN
- ACTi CAM-5200HP
- ACTi CAM-5201HN
- ACTi CAM-5201HP
- ACTi CAM-5220HN
- ACTi CAM-5220HP
- ACTi CAM-5221HN
- ACTi CAM-5221HP
- ACTi CAM-5300HN
- ACTi CAM-5300HP
- ACTi CAM-5301HN
- ACTi CAM-5301HP
- ACTi CAM-5320HN
- ACTi CAM-5320HP
- ACTi CAM-5321HN
- ACTi CAM-5321HP
- ACTi CAM-5322HN
- ACTi CAM-5322HP
- ACTi CAM-6200NN
- ACTi CAM-6200PN
- ACTi CAM-6220NN
- ACTi CAM-6220PN
- ACTi CAM-6220NW
- ACTi CAM-6220PW
- ACTi CAM-6500 NTSC
- ACTi CAM-6500 PAL
- ACTi CAM-6510 NTSC
- ACTi CAM-6510 PAL
- ACTi CAM-6520 NTSC
- ACTi CAM-6520 PAL
- ACTi CAM-6600 NTSC
- ACTi CAM-6600 PAL
- ACTi CAM-6610 NTSC
- ACTi CAM-6610 PAL
- ACTi CAM-6620 NTSC
- ACTi CAM-6620 PAL
- ACTi CAM-6630 NTSC
- ACTi CAM-6630 PAL
- ACTi CAM-7200N
- ACTi CAM-7200P
- ACTi CAM-7201N
- ACTi CAM-7201P
- ACTi CAM-7220N
- ACTi CAM-7220P
- ACTi CAM-7221N
- ACTi CAM-7221P
- ACTi CAM-7300N
- ACTi CAM-7300P
- ACTi CAM-7301N
- ACTi CAM-7301P
- ACTi CAM-7302N
- ACTi CAM-7302P
- ACTi CAM-7320N
- ACTi CAM-7320P
- ACTi CAM-7321N
- ACTi CAM-7321P
- ACTi CAM-7322N
- ACTi CAM-7322P
- ACTi CAM-7411
- ACTi TCM-4301
- ACTi TCM-5311

ApproTech

- APPRO LC-7211 PAL
- APPRO LC-7211 NTSC
- APPRO LC-7211W PAL
- APPRO LC-7211W NTSC
- APPRO LC-7214 PAL
- APPRO LC-7214 NTSC
- APPRO LC-7215 PAL
- APPRO LC-7215 NTSC
- APPRO LC-7221 PAL
- APPRO LC-7221 NTSC
- APPRO LC-7222 PAL
- APPRO LC-7222 NTSC
- APPRO LC-7222E PAL
- APPRO LC-7222E NTSC
- APPRO LC-7224E PAL
- APPRO LC-7224E NTSC
- APPRO LC-7225E PAL
- APPRO LC-7225E NTSC
- APPRO LC-7226 PAL
- APPRO LC-7226 NTSC
- APPRO LC-7228 PAL
- APPRO LC-7228 NTSC
- APPRO LC-7231 PAL
- APPRO LC-7231 NTSC
- APPRO LC-7222(E)
- APPRO LC-7222S(E)
- APPRO LC-7231HT
- APPRO LC-7314
- APPRO LC-7313
- APPRO LC-7233H

Arecont

- ARECONT AV1300
- ARECONT AV1300-AI
- ARECONT AV2100
- ARECONT AV2100-AI
- ARECONT AV3100
- ARECONT AV3100-AI
- ARECONT AV5100
- ARECONT AV5100-AI
- ARECONT AV1305
- ARECONT AV1305-AI
- ARECONT AV1305DN
- ARECONT AV2105
- ARECONT AV2105-AI
- ARECONT AV2105DN
- ARECONT AV1355
- ARECONT AV1355DN
- ARECONT AV2155
- ARECONT AV2155DN
- ARECONT AV3105
- ARECONT AV3105-AI
- ARECONT AV3105DN
- ARECONT AV3155
- ARECONT AV3155DN
- ARECONT AV5105
- ARECONT AV5105-AI

- ARECONT AV5105DN
- ARECONT AV5155
- ARECONT AV5155DN

Axis

- AXIS 205
- AXIS 206
- AXIS 206W
- AXIS 206M
- AXIS 207
- AXIS 207MW
- AXIS 207W
- AXIS 209FD
- AXIS 209FD-R
- AXIS 209MFD
- AXIS 209MFD-R
- AXIS 210
- AXIS 210A
- AXIS 211
- AXIS 211A
- AXIS 211M
- AXIS 211W
- AXIS 212 PTZ
- AXIS 212 PTZ-V
- AXIS 213 PTZ PAL
- AXIS 213 PTZ NTSC
- AXIS 214 PTZ PAL
- AXIS 214 PTZ NTSC
- AXIS 215 PTZ PAL
- AXIS 215 PTZ NTSC
- AXIS 215 PTZ-E NTSC
- AXIS 215 PTZ-E NTSC
- AXIS 216FD
- AXIS 216FD-V
- AXIS 216MFD
- AXIS 216MFD-V
- AXIS 221
- AXIS 223M
- AXIS 225FD
- AXIS 231D PAL
- AXIS 231D NTSC
- AXIS 231D+ PAL
- AXIS 231D+ NTSC
- AXIS 232D PAL
- AXIS 232D NTSC
- AXIS 232D+ PAL
- AXIS 232D+ NTSC
- AXIS 233D PAL
- AXIS 233D NTSC
- AXIS 2100
- AXIS 2110
- AXIS 2120 PAL
- AXIS 2120 NTSC
- AXIS 2130R PAL/NTSC
- AXIS 2420 PAL
- AXIS 2420 NTSC
- AXIS M1011
- AXIS M1011-W
- AXIS M1031-W
- AXIS M3011
- AXIS M3014
- AXIS P1311
- AXIS P3301
- AXIS P3301-V
- AXIS P3343
- AXIS P3343-V
- AXIS P3343-VE
- AXIS P3344
- AXIS P3344-V
- AXIS P3344-VE
- AXIS Q1755
- AXIS Q6032-E PAL
- AXIS Q6032-E NTSC

Eneo

- Eneo ENC-501L
- Eneo ENC-501W
- Eneo ENC-1001L
- Eneo ENC-1001W
- Eneo ENC-1002L
- Eneo ENC-1002W
- Eneo ENC-1003L
- Eneo ENC-1003W

Ernitec

- Ernitec ACM-1011
- Ernitec ACM-1231
- Ernitec ACM-1431
- Ernitec ACM-1511
- Ernitec ACM-3311
- Ernitec ACM-3411
- Ernitec ACM-3511
- Ernitec ACM-7411
- Ernitec ACM-4001
- Ernitec ACM-4201
- Ernitec CAM-6600
- Ernitec TCM-4301
- Ernitec EIP120C-P12P
- Ernitec EIP120D-P12P
- Ernitec EIP200D-P12P
- Ernitec EIP210C-P12P
- Ernitec EIP210D-P12P
- Ernitec EIP320DI-18E
- Ernitec EIP4200C-M
- Ernitec EIP510-C1
- Ernitec EIP5600C-M
- Ernitec EIP5600DN-M

General Electric

- GE Security GEC-IP2B
- GE Security GEC-IP2B-C
- GE Security GEC-IP2B-P
- GE Security GEC-IP2D
- GE Security GEC-IP2D-C
- GE Security GEC-IP2D-P
- GE Security GEC-IP2VD
- GE Security GEC-IP2VD-C
- GE Security GEC-IP2VD-P
- GE Security GEC-IP2VD-DN
- GE Security GEC-IP2VD-DNC
- GE Security GEC-IP2VD-DNP
- GE Security GEC-IPDRH-DN-POE NTSC
- GE Security GEC-IPDRH-DN-POE PAL
- GE Security GEC-IPDRH-DN-24VA NTSC
- GE Security GEC-IPDRH-DN-24VA PAL
- GE Security GEC-IPDRH-DN-24VA-P NTSC
- GE Security GEC-IPDRH-DN-24VA-P PAL
- GE Security GEC-IPDRH-POE NTSC
- GE Security GEC-IPDRH-POE PAL
- GE Security GEC-IPDRH-24VA NTSC
- GE Security GEC-IPDRH-24VA PAL
- GE Security GEC-IPDRH-24VA-P NTSC
- GE Security GEC-IPDRH-24VA-P PAL
- GE Security GEC-MP2
- GE Security GEC-MP3-DN

IQinVision

- IQeye IQ040Si-V9
- IQeye IQ041Si-V10
- IQeye IQ 042SI-V11
- IQeye IQ040S
- IQeye IQ041S
- IQeye IQ042S
- IQeye IQ301
- IQeye IQ301m
- IQeye IQ301w
- IQeye IQ302
- IQeye IQ302w
- IQeye IQ303
- IQeye IQ303w
- IQeye IQ501
- IQeye IQ510
- IQeye IQ511
- IQeye IQ601
- IQeye IQ602
- IQeye IQ603
- IQeye IQ701
- IQeye IQ702
- IQeye IQ703
- IQeye IQ705
- IQeye IQ710
- IQeye IQ711
- IQeye IQ712
- IQeye IQ751
- IQeye IQ752
- IQeye IQ753
- IQeye IQ755
- IQeye IQ811
- IQeye IQ802
- IQeye IQ803
- IQeye IQ805
- IQeye IQ851
- IQeye IQ852
- IQeye IQ853
- IQeye IQ855
- IQeye IQD41S
- IQeye IQ D42S
- IQeye IQ D40S
- IQeye IQA10S
- IQeye IQA10Si
- IQeye IQA10SE
- IQeye IQA20S
- IQeye IQA20Si
- IQeye IQA20SE
- IQeye IQA11S
- IQeye IQA11SE

- IQeye IQA11SI
- IQeye IQA12S
- IQeye IQA12SE
- IQeye IQA12SI
- IQeye IQA13S
- IQeye IQA13SE
- IQeye IQA13SI
- IQeye IQA15S
- IQeye IQA15SE
- IQeye IQA15SI
- IQeye IQA21S
- IQeye IQA21SE
- IQeye IQA21SI
- IQeye IQA22S
- IQeye IQA22SE
- IQeye IQA22SI
- IQeye IQA23S
- IQeye IQA23SE
- IQeye IQA23SI
- IQeye IQA25S
- IQeye IQA25SE
- IQeye IQA25SI
- IQeye IQD40SI-F1
- IQeye IQD41SI-F1
- IQeye IQD42SI-F1

Mobotix

- Mobotix D12Di-Sec-D43D43
- Mobotix D12Di-IT-DNight-D43N43
- Mobotix D12D-IT-DNight-D43N43
- Mobotix D22M-IT
- Mobotix D22M-Sec
- Mobotix D22M-IT-Night
- Mobotix D22M-Sec-Night
- Mobotix D24M-IT-D22
- Mobotix D24M-IT-Night
- Mobotix D24M-Sec
- Mobotix D24M-Sec-Night
- Mobotix D10Di-Night-D43N43
- Mobotix D10D-Night-D43N43
- Mobotix M12D-IT-Night-D43N43
- Mobotix M22M-Sec
- Mobotix M22M-Sec-Night
- Mobotix M22M-IT-D22
- Mobotix M22M-Sec-CSVario
- Mobotix M22M-Sec-Night-CSVario
- Mobotix M22M-IT
- Mobotix M22M-Night
- Mobotix M22M-Night-CS
- Mobotix M10Mi-Secure
- Mobotix M10D-Night D43 D135
- Mobotix M10D-Night D135 N135
- Mobotix M10M-IT D43
- Mobotix M10M-IT-D135
- Mobotix M10M-Secure D43
- Mobotix M10M-Sec-D135
- Mobotix M10M-Sec-N43
- Mobotix V10D

Panasonic

- PANASONIC BB-HCE481
- PANASONIC BB-HCE481A
- PANASONIC BB-HCM311
- PANASONIC BB-HCM311A
- PANASONIC BB-HCM331
- PANASONIC BB-HCM331A
- PANASONIC BB-HCM371
- PANASONIC BB-HCM371A
- PANASONIC BB-HCM381
- PANASONIC BB-HCM381A
- PANASONIC BB-HCM403
- PANASONIC BB-HCM403A
- PANASONIC BB-HCM511
- PANASONIC BB-HCM511A
- PANASONIC BB-HCM515
- PANASONIC BB-HCM515A
- PANASONIC BB-HCM527
- PANASONIC BB-HCM527A
- PANASONIC BB-HCM531
- PANASONIC BB-HCM531A
- PANASONIC BB-HCM547
- PANASONIC BB-HCM547A
- PANASONIC BB-HCM580
- PANASONIC BB-HCM580A
- PANASONIC BB-HCM581
- PANASONIC BB-HCM581A
- PANASONIC BB-HCM581A-W
- PANASONIC BB-HCM701
- PANASONIC BB-HCM701A
- PANASONIC BB-HCM705
- PANASONIC BB-HCM705A
- PANASONIC BB-HCM715
- PANASONIC BB-HCM715A
- PANASONIC BB-HCM735
- PANASONIC BB-HCM735A
- PANASONIC BL-C1
- PANASONIC BL-C1A
- PANASONIC BL-C10
- PANASONIC BL-C10A
- PANASONIC BL-C20
- PANASONIC BL-C20A
- PANASONIC BL-C30
- PANASONIC BL-C30A
- PANASONIC BL-C101
- PANASONIC BL-C101A
- PANASONIC BL-C111
- PANASONIC BL-C111A
- PANASONIC BL-C121
- PANASONIC BL-C121A
- PANASONIC BL-C131
- PANASONIC BL-C131A
- PANASONIC BL-C140
- PANASONIC BL-C140A
- PANASONIC BL-C160
- PANASONIC BL-C160A
- PANASONIC BL-C210
- PANASONIC BL-C210A
- PANASONIC BL-C230
- PANASONIC BL-C230A
- PANASONIC KX-HCM10
- PANASONIC KX-HCM8
- PANASONIC KX-HCM110
- PANASONIC KX-HCM 110A
- PANASONIC KX-HCM230
- PANASONIC KX-HCM250
- PANASONIC KX-HCMZ70
- PANASONIC KX-HCM280
- PANASONIC KX-HCM280A
- PANASONIC WV-NF284
- PANASONIC WV-NF302
- PANASONIC WV-NM100
- PANASONIC WV-NP240
- PANASONIC WV-NP244
- PANASONIC WV-NP304
- PANASONIC WV-NP472 PAL
- PANASONIC WV-NP472 NTSC
- PANASONIC WV-NW474S PAL
- PANASONIC WV-NW474S NTSC
- PANASONIC WV-NP502
- PANASONIC WV-NP1000
- PANASONIC WV-NP1004
- PANASONIC WV-NS202
- PANASONIC WV-NS202A
- PANASONIC WV-NS320 PAL
- PANASONIC WV-NS324 PAL
- PANASONIC WV-NS324 NTSC
- PANASONIC WV-NS950
- PANASONIC WV-NS954
- PANASONIC WV-NW470S PAL
- PANASONIC WV-NW484S
- PANASONIC WV-NW960
- PANASONIC WV-NW964

Sony

- SONY SNC-CS3N
- SONY SNC-CS3P
- SONY SNC-CS10
- SONY SNC-CS11
- SONY SNC-CS50N
- SONY SNC-CS50P
- SONY SNC-DF40N
- SONY SNC-DF40P
- SONY SNC-DF50N
- SONY SNC-DF50P
- SONY SNC-DF70N
- SONY SNC-DF70P
- SONY SNC-DF80N
- SONY SNC-DF80P
- SONY SNC-P1
- SONY SNC-P5
- SONY SNC-RZ25N
- SONY SNC-RZ25P
- SONY SNC-RZ30N
- SONY SNC-RZ30P
- SONY SNC-RZ50N
- SONY SNC-RZ50P
- SONY SNC-Z20N
- SONY SNC-Z20P
- SONY SNC-RX530N
- SONY SNC-RX530P
- SONY SNC-RX550N
- SONY SNC-RX550P
- SONY SNC-RX570N
- SONY SNC-RX570P

Toshiba
- TOSHIBA IK-WB01
- TOSHIBA IK-WB01A
- TOSHIBA IK-WB02
- TOSHIBA IK-WB02A
- TOSHIBA IK-WB11
- TOSHIBA IK-WB11A
- TOSHIBA IK-WB15A
- TOSHIBA IK-WB21A
- TOSHIBA IK-WR01A

Videoline
- Videoline EYE-P 11
- Videoline EYE-P 14
- Videoline EYE-P 15
- Videoline EYE-P 21

WebCAM
- WebCAM 1100A PAL
- WebCAM 1100A NTSC
- WebCAM 1100A-D PAL
- WebCAM 1100A-D NTSC
- WebCAM 1101A PAL
- WebCAM 1101A NTSC
- WebCAM 1101A-D PAL
- WebCAM 1101A-D NTSC
- WebCAM 3100A PAL
- WebCAM 3100A NTSC
- WebCAM 3100A-D PAL
- WebCAM 3100A-D NTSC
- WebCAM 3101A PAL
- WebCAM 3101A NTSC
- WebCAM 3101A-D PAL
- WebCAM 3101A-D NTSC
- WebCAM 3500A PAL
- WebCAM 3500A NTSC
- WebCAM 3500A-D NTSC
- WebCAM 3500A-D PAL
- WebCAM 3501A PAL
- WebCAM 3501A NTSC
- WebCAM 3501A-D PAL
- WebCAM 3501A-D NTSC

Xenics
- Xenics Gobi 384

Zavio
- Zavio D510E
- Zavio D520E
- Zavio D610A NTSC
- Zavio D610A PAL
- Zavio D611E NTSC
- Zavio D611E PAL
- Zavio F210A
- Zavio F312A
- Zavio F510E
- Zavio F510W
- Zavio F511E
- Zavio F511W
- Zavio F520E
- Zavio F521E
- Zavio F610A NTSC
- Zavio F610A PAL
- Zavio F611E NTSC
- Zavio F611E PAL
- Zavio F721A NTSC
- Zavio F721A PAL
- Zavio F731E
- Zavio N6130 NTSC
- Zavio N6130 PAL
- Zavio N6630
- Zavio N6720 NTSC
- Zavio N6720 PAL
- Zavio N7000
- Zavio N7130 NTSC
- Zavio N7130 PAL
- Zavio M510E
- Zavio M510W
- Zavio M511E
- Zavio M511W
- Zavio N1000
- Zavio N1250
- Zavio N2030
- Zavio N2060
- Zavio N2230
- Zavio N2260
- Zavio N6030
- Zavio N6031
- Zavio N6060
- Zavio N6230
- Zavio N6260
- Zavio N6600

Network Video Servers

1-port video servers:
- ACTi ACD-2100 NTSC
- ACTi ACD-2100 PAL
- ACTi SED-2120 NTSC
- ACTi SED-2120 PAL
- ACTi SED-2120S NTSC
- ACTi SED-2120S PAL
- ACTi SED-2120T NTSC
- ACTi SED-2120T PAL
- ACTi SED-2140 NTSC
- ACTi SED-2140 PAL
- ACTi SED-2140S NTSC
- ACTi SED-2140S PAL
- ACTi SED-2140T NTSC
- ACTi SED-2140T PAL
- APPRO VS-2112B NTSC
- APPRO VS-2112B PAL
- APPRO VS-2112T PAL
- APPRO VS-2112T NTSC
- APPRO VS-2311TE
- AXIS 241S Single Channel Video Server
- AXIS 241SA Single Channel Video Server
- AXIS 242S IV Single Channel Video Server
- AXIS 243SA Single Channel Video Server
- AXIS 247S Single Channel Video Server PAL
- AXIS 247S Single Channel Video Server NTSC
- AXIS Q7401 Single Channel Video Server PAL
- AXIS Q7401 Single Channel Video Server NTSC
- AXIS M7001 Video Encoder
- PANASONIC BB-HCS301A Single Channel Video Server
- WebCCTV NVE 1000
- Zavio V111T PAL
- Zavio V111T NTSC
- Zavio N5010 PAL
- Zavio N5010 NTSC

2-port video servers:
- WebCCTV NVE 2000

4-port video servers:
- WebCCTV NVS 400
- WebCCTV NVE 4000

Digitisers
- GuardDVR-4
- GuardDVR-8
- GuardDVR-16
- GuardDVR-20

Analogue Dome Cameras*

BBV protocol, Bosch, Kalatel; LG; Panasonic; Pelco; Sanyo; Siemens; Vicon; WebCCTV

* Analogue cameras support depends on the selected Network Video Server